Deployment Report for MI-636-51

Report Version:	Version 0.2.0
Created:	28.11.2025 16:13:23

System Information

Hostname:	MI-636-51
System Type:	x64-based PC
Manufacturer:	Microsoft Corporation
Model:	Virtual Machine
Serial Number:	8933-8122-2268-6602-8470-6636-51
CPU 0	<table><tr><td>CPU:</td><td>Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz</td></tr><tr><td>CPU Cores:</td><td>1</td></tr><tr><td>Logical Procs:</td><td>2</td></tr></table>
RAM:	8,00 GB
OS:	Microsoft Windows 11 Enterprise LTSC
OS Version:	24H2
OS Build:	10.0.26100
OS ReleaseID:	2009

OS Security Configuration

User Account Control

Implemented Setting:	UAC is enabled.
Expected Setting:	UAC is enabled.
Description:	UAC improves the security of Windows devices by limiting the access that malicious code has to execute with administrator privileges. UAC empowers users to make informed decisions about actions that might affect the stability and security of their device.

SSL/TLS Configuration

SSL 2.0 Configuration

Implemented Setting:	SSL 2.0 Client is disabled.
Implemented Setting:	SSL 2.0 Client is disabled by default.
Implemented Setting:	SSL 2.0 Server is disabled.
Implemented Setting:	SSL 2.0 Server is disabled by default.

SSL 3.0 Configuration

Implemented Setting:	SSL 3.0 Client is disabled.
Implemented Setting:	SSL 3.0 Client is disabled by default.
Implemented Setting:	SSL 3.0 Server is disabled.
Implemented Setting:	SSL 3.0 Server is disabled by default.

TLS 1.0 Configuration

Implemented Setting:	TLS 1.0 Client is disabled.
Implemented Setting:	TLS 1.0 Client is disabled by default.

Implemented Setting:	TLS 1.0 Server is disabled.
Implemented Setting:	TLS 1.0 Server is disabled by default.

TLS 1.1 Configuration

Implemented Setting:	TLS 1.1 Client is disabled.
Implemented Setting:	TLS 1.1 Client is disabled by default.
Implemented Setting:	TLS 1.1 Server is disabled.
Implemented Setting:	TLS 1.1 Server is disabled by default.

TLS 1.2 Configuration

Implemented Setting:	TLS 1.2 Client is enabled.
Implemented Setting:	TLS 1.2 Client is enabled by default.
Implemented Setting:	TLS 1.2 Server is enabled.
Implemented Setting:	TLS 1.2 Server is enabled by default.

TLS 1.3 Configuration

Implemented Setting:	TLS 1.3 Client is enabled.
Implemented Setting:	TLS 1.3 Client is enabled by default.
Implemented Setting:	TLS 1.3 Server is enabled.
Implemented Setting:	TLS 1.3 Server is enabled by default.

Certificate Padding Check Configuration

Implemented Setting:	Certificate Padding Check is enabled.
Expected Setting:	Certificate Padding Check should be enabled.
Description:	This setting controls whether the padding check is enabled or disabled during the validation of certificates. Padding is a mechanism used in

	cryptography to adjust data to a specific length required by encryption algorithms. In the case of certificates, padding may be necessary to adjust the data to a certain block size. The padding check ensures that no insecure or incorrect padding values are present in the certificates, which could lead to security vulnerabilities.

TLS Cipher Suite Configuration

Name	Status
Cipher 'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_RSA_WITH_AES_256_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_RSA_WITH_AES_128_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_RSA_WITH_3DES_EDE_CBC_SHA'	Is disabled. ✅
Cipher 'TLS_RSA_WITH_NULL_SHA'	Is disabled. ✅
Cipher 'TLS_DHE_RSA_WITH_AES_256_CBC_SHA'	Is disabled. ✅

Cipher 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA'	Is disabled.
Cipher 'TLS_DHE_DSS_WITH_AES_256_CBC_SHA'	Is disabled.
Cipher 'TLS_DHE_DSS_WITH_AES_128_CBC_SHA'	Is disabled.
Cipher 'TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA'	Is disabled.
Cipher 'TLS_RSA_WITH_RC4_128_SHA'	Is disabled.
Cipher 'TLS_RSA_WITH_RC4_128_MD5'	Is disabled.
Cipher 'TLS_RSA_WITH_DES_CBC_SHA'	Is disabled.
Cipher 'TLS_DHE_DSS_WITH_DES_CBC_SHA'	Is disabled.
Cipher 'TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA'	Is disabled.
Cipher 'TLS_RSA_WITH_NULL_MD5'	Is disabled.
Cipher 'TLS_RSA_EXPORT1024_WITH_RC4_56_SHA'	Is disabled.
Cipher 'TLS_RSA_EXPORT_WITH_RC4_40_MD5'	Is disabled.
Cipher 'TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA'	Is disabled.

Link-Local Multicast Resolution (LLMNR) Configuration

Implemented Setting:	Link-Local Multicast Resolution (LLMNR) is disabled. ✅
Expected Setting:	Link-Local Multicast Resolution (LLMNR) should be disabled.
Description:	Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

WDigest Credential Caching Configuration

Implemented Setting:	WDigest Credential Caching is disabled. ✅
Expected Setting:	WDigest Credential Caching should be disabled.
Description:	WDigest Caching is an old technology (but still used) used to store (cache) the passwords of the logged in users in the memory and use it to negotiate the authentication on the network.

LSASS Configuration

Implemented Setting:	LSASS is running as a protected process. ✅
Expected Setting:	LSASS should be running as a protected process.
Description:	This feature aims to prevent unauthorized access, memory reading, and code injection by non-protected processes. By enabling LSA protection, administrators can reinforce the security measures surrounding user credentials, ensuring that they remain confidential and safeguarded against potential threats.

SMBv1 Configuration

Implemented Setting:	SMB1Protocol-Deprecation is not installed. ✅
Implemented Setting:	SMB1Protocol is not installed. ✅
Implemented Setting:	SMB1Protocol-Client is not installed. ✅
Implemented Setting:	SMB1Protocol-Server is not installed. ✅
Expected Setting:	SMBv1 Features should not be installed.
Description:	SMB (Server Message Block) is a network-layered protocol mainly used on Windows for sharing files, printers, and communication between network-attached computers.

SMBv3 Configuration

Implemented Setting:	SMBv3 Signature configuration is active. ✅
Implemented Setting:	SMBv3 Encryption configuration is active. ✅
Implemented Setting:	SMBv3 Security configuration is active. ✅

Built-in Administrator Account

Implemented Setting:	The Built-in 'Administrator' user account is disabled. ✅
Expected Setting:	The Built-in 'Administrator' user account should be disabled.
Description:	The built-in administrator account has a specific and well-known security identifier, and some attacks target that particular SID. Renaming the account doesn't help, because the SID will stay the same. Therefore, the BuiltIn Administrator account should be disbaled.

Local Administrator Password Settings

Implemented Setting:	User sysadmin has 'Password never expires' set to true. ✅
Expected Setting:	The 'Password never expires' setting should be set to true.
Description:	Setting “Password never expires” for a local user ensures that the account remains accessible without forced password changes. This is especially important for system service accounts, deployment accounts, or automated maintenance users, where password expiration could break scripts, scheduled tasks, or critical services. It prevents unexpected lockouts and keeps automated processes running reliably.

Remote Desktop Protocol Settings

Implemented Setting:	Remote Desktop Protocol is enabled. ✅
Expected Setting:	The Remote Desktop Protocol should be enabled.
Description:	Remote Desktop Protocol is used to connect to a PC from a remote device by using the Microsoft Remote Desktop client. RDP Sessions are secured by Group Policy Settings in a domain.

RDP Authentication Settings

Implemented Setting:	RDP Network-Level user authentication is disabled. ✅
Expected Setting:	RDP Network-Level user authentication should be disabled.
Description:	RDP Network-Level user authentication restricts access to the PC. If enabled, users have to authenticate themselves to the network before they can connect to the PC. This makes no sense in this state of implementation of the PC. RDP Sessions are secured by Group Policy Settings in a domain.

Location Service

Implemented Setting:	Location Service is disabled. ✅
Expected Setting:	Location Service should be disabled.
Description:	If enabled, Windows will use the device's capabilities to determine your location and will use this location data. This information is provided to 3rd party applications and services. So we recommend to turn this off by default.

New Network Window

Implemented Setting:	Network Localization for 'New Network Window' is disabled. ✅
Expected Setting:	Network Localization for 'New Network Window' should be disabled.
Description:	By default, the first time you connect to a new network (wired or wireless), you will be prompted "Do you want to allow your PC to be discoverable by other PCs and devices on this network?" by the Network Location wizard. So we recommend to turn this off by default.

WinRM Service Status

Implemented Setting:	Windows-Remoteverwaltung (WS-Verwaltung) - WinRM is up and running. ✅
Expected Setting:	Windows-Remoteverwaltung (WS-Verwaltung) - WinRM should be enabled and running.
Description:	We need WinRM in our environments for automatization tools like Software deployment and updates/upgrades to do these jobs remotely. Securtity settings are made via GPO settings in domain.

SNMP Windows Feature on Demand

Name: Simple Network Management-Protokoll (SNMP)

Description: The Microsoft Windows implementation of the Simple Network Management Protocol (SNMP) is used to configure remote devices, monitor network performance, audit network usage, and detect network faults or inappropriate access.

Status Enabled: SNMP FoD is installed.

Firewall Configuration

RDP Firewall Rules

Status	Name	Group	Description
True	Remotedesktop - Schatten (TCP eingehend)	Remotedesktop	Eingehende Regel f�r den Remotedesktopdienst, um das Spiegeln einer vorhandenen Remotedesktopsitzung zuzulassen. (TCP eingehend)
True	Remotedesktop - Benutzermodus (TCP eingehend)	Remotedesktop	Eingehende Regel f�r den Remotedesktopdienst, die RDP-Datenverkehr zul�sst. [TCP 3389]
True	Remotedesktop - Benutzermodus (UDP eingehend)	Remotedesktop	Eingehende Regel f�r den Remotedesktopdienst, die RDP-Datenverkehr zul�sst [UDP 3389]

ICMP v4 Firewall Rules

Status	Name	Description
True	ICMP Allow incoming V4 echo request	Incoming ICMP V4 echo requests are allowed in 'Any' profile through local firewall.

Windows Firewall Status

Scope	Enabled
Domain	True

Private	True
Public	True

OS Adjustments

IPv6 Network Setting

Implemented Setting:	IPv6 on Network Adapter 'Ethernet' is disabled. ✅
Expected Setting:	IPv6 on Network Adapter '' should be disabled.
Description:	Due to troubleshooting network issues and to guarantee proper network functionality with all our services, we disable IPv6 on our network adapters.

First Logon Animation

Implemented Setting:	The 'First Logon Animation' is disabled. ✅
Expected Setting:	The 'First Logon Animation' should be disabled.
Description:	To reduce the time the deployment takes to finish and speed up the overall logon procedure, we disable the first logon animation.

Delayed Desktop Switch

Implemented Setting:	The 'Delayed Desktop Switch' is disabled. ✅
Expected Setting:	The 'Delayed Desktop Switch' should be disabled.
Description:	To reduce the time the deployment takes to finish and speed up the overall logon procedure, we disable the 'Delayed Desktop Switch'.

WSUS Information

Windows Update Server: http://wsussrv1:8530

Status Server: http://wsussrv1:8530

NonAdmins Elevation: Not Set.

Do Not Connect to Microsoft Windows Update Internet Locations: Not Set.

Set Update Notification Level: Not Set.

Update Notification Level: Not Set.

WSUS Advanced Settings

Automatic Update Options: Not Set.

Windows Update Settings: The client connects to the specified local update service (WSUS).

Atomatic Reboot while Users are logged on: Not Set.

Automatic Update Setting: Not Set.

Setting on which day updates will be installed: Not Set.

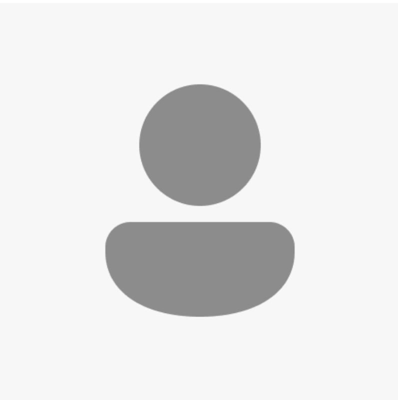
Setting when updates will be installed on a specific day: This setting is not configred.

OEM Information

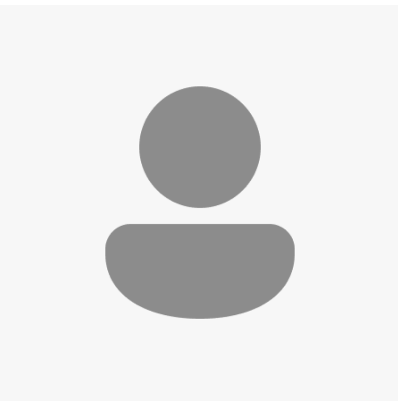
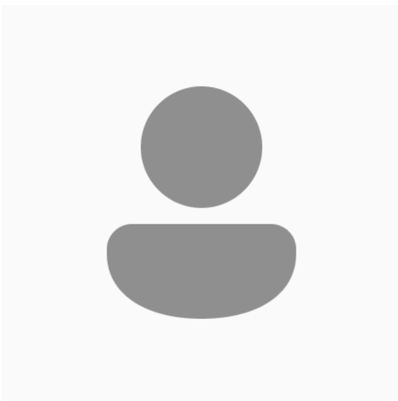
OEM Image 'Powershell_oem.bmp' is available under 'C:\windows\system32\'.

OEM User Account Image 'Powershell_oem.bmp' is available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

Guest User Account Images 'guest.bmp' and 'guest.png' are available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

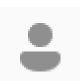
 

Guest User Account Images 'user.bmp' and 'user.png' are available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

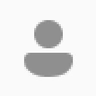
 

Guest User Account Image 'user-32.png' is available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

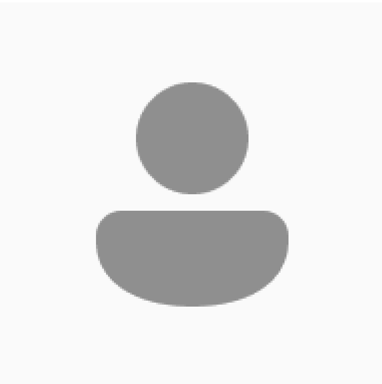
Guest User Account Image 'user-40.png' is available in 'C:\ProgramData\Microsoft\User Account Pictures\'.



Guest User Account Image 'user-48.png' is available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

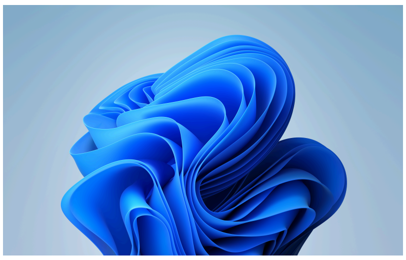


Guest User Account Image 'user-192.png' is available in 'C:\ProgramData\Microsoft\User Account Pictures\'.

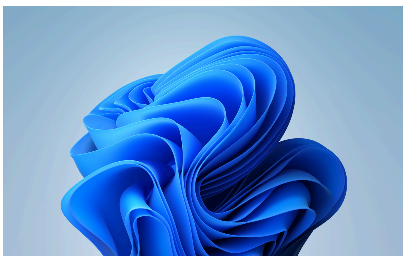


OEM Image 'Powershell_oem.bmp' is available in 'C:\windows\system32\oobe\info\'.

OEM Wallpaper 'Wallpaper.jpg' is available in 'C:\windows\system32\oobe\info\backgrounds\'.



OEM Wallpaper 'Wallpaper.jpg' is available in 'C:\Windows\Web\Wallpaper\Windows\'.



OEM Registry Values

Manufacturer: Lorem Ipsum

Logo: C:\Windows\System32\Powershell_oem.bmp

PowerPlan Settings

Name: Ausbalanciert

Description: Stellt automatisch einen Ausgleich zwischen Leistung und Stromverbrauch der Hardware her, die diese Funktion unterst�tzt.

Status Enabled: True

PowerPlan Options

Name	Plugged in Power Setting	On Battery Power Setting
Monitor Timeout	300 Minutes	3 Minutes
Disk Timeout	Deactivated	10 Minutes
Standby Timeout	Deactivated	10 Minutes
Hibernate Timeout	Deactivated	Deactivated
USB Selective Suspend	Deactivated	Activated

Storage Information

System Storage Information

Volume Name	Drive Letter	File System	Drive Type	Status	Operational	Max Useable Size
Recovery		NTFS	Fixed	Healthy	OK	0.49 GB
Windows	C	NTFS	Fixed	Healthy	OK	146.48 GB
BOOT		FAT32	Fixed	Healthy	OK	0.48 GB
Data	D	NTFS	Fixed	Healthy	OK	52.41 GB

BitLocker Status Information

Mount Point	Volume Type	Protection Status
C:	OperatingSystem	Off
D:	Data	Off

VSS Settings

Maximum VSS Setting for Volume 'C:': Max. Schattenkopie-Speicherbereich: 7,32 GB (5%)

Maximum VSS Setting for Volume 'D:': Max. Schattenkopie-Speicherbereich: 5,24 GB (10%)

Local User & Groups

Local User Information

Name	Enabled	Description
Administrator	False	Vordefiniertes Konto f�r die Verwaltung des Computers bzw. der Dom�ne
DefaultAccount	False	Ein vom System verwaltetes Benutzerkonto.
Gast	False	Vordefiniertes Konto f�r Gastzugriff auf den Computer bzw. die Dom�ne
sysadmineuro	True	Eurofunk Systemadministrator
WDAGUtilityAccount	False	Ein Benutzerkonto, das vom System f�r Windows Defender Application Guard-Szenarien verwaltet und verwendet wird

Local Group Information

Name	Description

Administratoren	Administratoren haben uneingeschr�nkten Vollzugriff auf den Computer bzw. die Dom�ne.
Benutzer	Benutzer k�nnen keine zuf�lligen oder beabsichtigten �nderungen am System durchf�hren und d�rfen die meisten herk�mmlichen Anwendungen ausf�hren.
Benutzermodus-Hardwareoperatoren	Mitglieder dieser Gruppe k�nnen Hardware aus dem Benutzermodus betreiben.
Distributed COM-Benutzer	Mitglieder dieser Gruppe k�nnen Distributed-COM-Objekte auf diesem Computer starten, aktivieren und verwenden.
Ereignisprotokollleser	Mitglieder dieser Gruppe d�rfen Ereignisprotokolle des lokalen Computers lesen
Ger�tebesitzer	Mitglieder dieser Gruppe k�nnen systemweite Einstellungen �ndern.
G�ste	G�ste besitzen standardm��ig die selben Zugriffsrechte wie Mitglieder der Benutzergruppe. Das Gastkonto ist jedoch zus�tzlich eingeschr�nkt.
Hauptbenutzer	"Hauptbenutzer" sind eingeschlossen aus Gr�nden der R�ckw�rtskompatibilit�t, sie besitzen eingeschr�nkte administrative Rechte.
Hyper-V-Administratoren	Die Mitglieder dieser Gruppe erhalten uneingeschr�nkten Zugriff auf s�mtliche Features von Hyper-V.
IIS_IUSRS	Von Internetinformationsdiensten verwendete integrierte Gruppe.

Kryptografie-Operatoren	Die Mitglieder sind berechtigt, kryptographische Vorg�nge durchzuf�hren.
Leistungsprotokollbenutzer	Mitglieder dieser Gruppe k�nnen die Protokollierung von Leistungsindikatoren planen, Traceanbieter aktivieren und Ereignistraces sammeln, sowohl lokal als auch �ber Remotezugriff auf diesen Computer.
Leistungs�berwachungsbenutzer	Mitglieder dieser Gruppe k�nnen lokal und remote auf Leistungsz�hlerdaten zugreifen
Netzwerkkonfigurations-Operatoren	Mitglieder dieser Gruppe verf�gen �ber einige Administratorrechte zum Verwalten der Konfiguration von Netzwerkfeatures.
OpenSSH-Benutzer	Mitglieder dieser Gruppe k�nnen �ber SSH. eine Verbindung mit diesem Computer herstelle
Remotedesktopbenutzer	Mitglieder dieser Gruppe haben die Berechtigung, sich remote anzumelden.
Remoteverwaltungsbenutzer	Mitglieder dieser Gruppe k�nnen �ber Verwaltungsprotokolle auf WMI-Ressourcen zugreifen (z. B. WS-Verwaltung �ber den Windows-Remoteverwaltungsdienst). Dies gilt nur f�r WMI-Namespaces, die dem Benutzer Zugriff gew�hren.
Replikations-Operator	Unterst�tzt Dateireplikation in Dom�nen.
Sicherungs-Operatoren	Sicherungs-Operatoren k�nnen Sicherheitseinschr�nkungen lediglich zum Sichern oder Wiederherstellen von Dateien au�er Kraft setzen.

System Managed Accounts Group	Die Mitglieder dieser Gruppe werden vom System verwaltet.
Zugriffssteuerungs-Unterst�tzungsoperatoren	Mitglieder dieser Gruppe k�nnen remote Autorisierungsattribute und -berechtigungen f�r Ressourcen auf dem Computer abfragen.

Software & Windows Features

Installed Software

Installed Programs

Name	Version	Vendor
Microsoft Edge	142.0.3595.94	Microsoft Corporation
Microsoft Edge WebView2-Laufzeit	142.0.3595.94	Microsoft Corporation

System Services

Default Active Services

State	Name	Display Name
Running	Appinfo	Anwendungsinformationen
Running	AppXSvc	AppX-Bereitstellungsdienst (AppXSVC)
Running	AudioEndpointBuilder	Windows-Audio-Endpunkterstellung
Running	Audiosrv	Windows-Audio
Running	BFE	Basisfiltermodul
Running	BrokerInfrastructure	Infrastrukturdienst f�r Hintergrundaufgaben

Running	camsvc	Manager-Dienst f�r den Funktionszugriff
Running	cbdhsvc_603910	Zwischenablage-Benutzerdienst_603910
Running	CDPSvc	Plattformdienst f�r verbundene Ger�te
Running	CDPUserSvc_603910	Benutzerdienst f�r die Plattform f�r verbundene Ger�te_603910
Running	CertPropSvc	Zertifikatverteilung
Running	CoreMessagingRegistrar	CoreMessaging
Running	CryptSvc	Kryptografiedienste
Running	DcomLaunch	DCOM-Server-Prozessstart
Running	Dhcp	DHCP-Client
Running	DiagTrack	Benutzererfahrungen und Telemetrie im verbundenen Modus
Running	DispBrokerDesktopSvc	Anzeigerichtliniendienst
Running	Dnscache	DNS-Client
Running	DoSvc	�bermittlungsoptimierung
Running	DPS	Diagnoserichtliniendienst
Running	DsSvc	Datenfreigabedienst
Running	DusmSvc	Datennutzung
Running	EventLog	Windows-Ereignisprotokoll
Running	EventSystem	COM+-Ereignissystem
Running	FontCache	Windows-Dienst f�r Schriftartencache
Running	gpsvc	Gruppenrichtlinienclient
Running	InstallService	Microsoft Store-Installationsdienst
Running	InventorySvc	Inventur- und Kompatibilit�tssentit�tsdienst
Running	iphlpsvc	IP-Hilfsdienst

Running	KeyIso	CNG-Schl�sselisolation
Running	LanmanServer	Server
Running	LanmanWorkstation	Arbeitsstationsdienst
Running	lfsvc	Geolocation-Dienst
Running	LicenseManager	Windows-Lizenz-Manager-Dienst
Running	LSM	Lokaler Sitzungs-Manager
Running	MDCoreSvc	Microsoft Defender Core-Dienst
Running	mpssvc	Windows Defender Firewall
Running	NcbService	Netzwerkverbindungsbroker
Running	netprofm	Netzwerklistendienst
Running	NetSetupSvc	Netzwerkeinrichtungsdienst
Running	nsi	Netzwerkspeicher-Schnittstellendienst
Running	OneSyncSvc_603910	Synchronisierungshost_603910
Running	PcaSvc	Programmkompatibilit�ts-Assistent-Dienst
Running	PimIndexMaintenanceSvc_603910	Kontaktdaten_603910
Running	PlugPlay	Plug & Play
Running	Power	Stromversorgung
Running	ProfSvc	Benutzerprofildienst
Running	RmSvc	Funkverwaltungsdienst
Running	RpcEptMapper	RPC-Endpunktzuordnung
Running	RpcSs	Remoteprozeduraufruf (RPC)
Running	SamSs	Sicherheitskonto-Manager
Running	Schedule	Aufgabenplanung
Running	seclogon	Sekund�re Anmeldung
Running	SecurityHealthService	Windows-Sicherheitsdienst

Running	SENS	Benachrichtigungsdienst f�r Systemereignisse
Running	SessionEnv	Konfiguration f�r Remotedesktops
Running	ShellHWDetection	Shellhardwareerkennung
Running	smphost	Microsoft-SMP f�r Speicherpl�tze
Running	SNMP	SNMP-Dienst
Running	Spooler	Druckwarteschlange
Running	SSDPSRV	SSDP-Suche
Running	StateRepository	StateRepository-Dienst
Running	StorSvc	Speicherdienst
Running	swprv	Microsoft-Softwareschattenkopie-Anbieter
Running	SysMain	SysMain
Running	SystemEventsBroker	Systemereignissebroker
Running	TermService	Remotedesktopdienste
Running	TextInputManagementService	Texteingabeverwaltungsdienst
Running	Themes	Designs
Running	TimeBrokerSvc	Zeitbroker
Running	TokenBroker	Web Account Manager
Running	TrkWks	�berwachung verteilter Verkn�pfungen (Client)
Running	TrustedInstaller	Windows Modules Installer
Running	UdkUserSvc_603910	Udk-Benutzerdienst_603910
Running	UmRdpService	Anschlussumleitung f�r Remotedesktopdienst im Benutzermodus
Running	UnistoreSvc_603910	Benutzerdatenspeicher _603910
Running	UserDataSvc_603910	Benutzerdatenzugriff_603910
Running	UserManager	Benutzer-Manager

Running	UsoSvc	Update Orchestrator Service
Running	VaultSvc	Anmeldeinformationsverwaltung
Running	vmicheartbeat	Hyper-V-Taktdienst
Running	vmickvpexchange	Hyper-V-Datenaustauschdienst
Running	vmicrdv	Hyper-V-Remotedesktopvirtualisierungsdienst
Running	vmicshutdown	Hyper-V-Dienst zum Herunterfahren des Gasts
Running	vmicvss	Hyper-V-Volumeschattenkopie-Anforderer
Running	VSS	Volumeschattenkopie
Running	Wcmsvc	Windows-Verbindungs-Manager
Running	WdNisSvc	Microsoft Defender Antivirus-Netzwerkinspektionsdienst
Running	webthreatdefsvc	Web Threat Defense-Dienst
Running	webthreatdefusersvc_603910	Web Threat Defense-Benutzerdienst_603910
Running	whesvc	Windows-Integrit�t und optimierte Oberfl�chen
Running	WinDefend	Microsoft Defender Antivirus-Dienst
Running	WinHttpAutoProxySvc	WinHTTP-Web Proxy Auto-Discovery-Dienst
Running	Winmgmt	Windows-Verwaltungsinstrumentation
Running	WinRM	Windows-Remoteverwaltung (WS-Verwaltung)
Running	WpnService	Windows-Pushbenachrichtigungssystemdienst
Running	WpnUserService_603910	Windows-Pushbenachrichtigungs-Benutzerdienst_603910
Running	WSAIFabricSvc	WSAIFabricSvc
Running	wscsvc	Sicherheitscenter

Running	WSearch	Windows Search

Installed Drivers

Installed Drivers

Device Name	Manufacturer	Driver Version
ACPI Module Device	(Standard system devices)	10.0.26100.1150
ACPI x64-based PC	(Standard computers)	10.0.26100.1
Advanced programmable interrupt controller	(Standard system devices)	10.0.26100.1150
Audio Endpoint	Microsoft	10.0.26100.1
Composite Bus Enumerator	Microsoft	10.0.26100.1150
Computer Device	Microsoft	10.0.26100.1
Disk drive	(Standard disk drives)	10.0.26100.7019
Generic PnP Monitor	(Standard monitor types)	10.0.26100.7019
Generic PnP Monitor	(Standard monitor types)	10.0.26100.7019
Generic software device	Microsoft	10.0.26100.1
Generic software device	Microsoft	10.0.26100.1
Generic software device	Microsoft	10.0.26100.1
Generic software device	Microsoft	10.0.26100.1
Generic volume shadow copy	Microsoft	10.0.26100.1
HID-compliant mouse	Microsoft	10.0.26100.1150
Intel Processor	Intel	10.0.26100.7019
Intel Processor	Intel	10.0.26100.7019

Local Print Queue	Microsoft	10.0.26100.1
Local Print Queue	Microsoft	10.0.26100.1
Local Print Queue	Microsoft	10.0.26100.1
Local Print Queue	Microsoft	10.0.26100.1
Microsoft ACPI-Compliant System	Microsoft	10.0.26100.7019
Microsoft Basic Display Driver	(Standard display types)	10.0.26100.4202
Microsoft Basic Render Driver	Microsoft	10.0.26100.7019
Microsoft Hyper-V Activation Component	Microsoft	10.0.26100.1
Microsoft Hyper-V Data Exchange	Microsoft	10.0.26100.1
Microsoft Hyper-V Dynamic Memory	Microsoft	10.0.26100.5074
Microsoft Hyper-V Generation Counter	Microsoft	10.0.26100.1150
Microsoft Hyper-V Guest Shutdown	Microsoft	10.0.26100.1
Microsoft Hyper-V Heartbeat	Microsoft	10.0.26100.1
Microsoft Hyper-V Input	Microsoft	10.0.26100.1150
Microsoft Hyper-V Network Adapter	Microsoft	10.0.26100.7019
Microsoft Hyper-V Remote Desktop Control Channel	Microsoft	10.0.26100.1
Microsoft Hyper-V Remote Desktop Virtualization	Microsoft	10.0.26100.1
Microsoft Hyper-V SCSI Controller	Microsoft	10.0.26100.6725
Microsoft Hyper-V Video	Microsoft	10.0.26100.1150
Microsoft Hyper-V Virtual Keyboard	Microsoft	10.0.26100.1150

Microsoft Hyper-V Virtual Machine Bus	Microsoft	10.0.26100.7019
Microsoft Hyper-V Virtualization Infrastructure Driver	Microsoft	10.0.26100.7019
Microsoft Hyper-V Volume Shadow Copy	Microsoft	10.0.26100.1
Microsoft Kernel Debug Network Adapter	Microsoft	10.0.26100.3624
Microsoft Remote Display Adapter	Microsoft	10.0.26100.7019
Microsoft Storage Spaces Controller	Microsoft	10.0.26100.7171
Microsoft System Management BIOS Driver	(Standard system devices)	10.0.26100.1
Microsoft Virtual Drive Enumerator	Microsoft	10.0.26100.1591
NDIS Virtual Network Adapter Enumerator	Microsoft	10.0.26100.1
Plug and Play Software Device Enumerator	(Standard system devices)	10.0.26100.4202
Remote Desktop Device Redirector Bus	Microsoft	10.0.26100.1150
Remote Desktop Keyboard Device	(Standard system devices)	10.0.26100.1150
Remote Desktop Mouse Device	(Standard system devices)	10.0.26100.1
Remote Desktop USB Hub	(Standard system devices)	10.0.26100.1150
System CMOS/real time clock	(Standard system devices)	10.0.26100.1150
UMBus Enumerator	Microsoft	10.0.26100.1150
UMBus Enumerator	Microsoft	10.0.26100.1150
UMBus Enumerator	Microsoft	10.0.26100.1150
UMBus Enumerator	Microsoft	10.0.26100.1150

UMBus Root Bus Enumerator	Microsoft	10.0.26100.1150
Volume	Microsoft	10.0.26100.5074
Volume	Microsoft	10.0.26100.5074
Volume	Microsoft	10.0.26100.5074
Volume	Microsoft	10.0.26100.5074
Volume	Microsoft	10.0.26100.5074
Volume Manager	Microsoft	10.0.26100.7019