CONFIGURATION AUDIT MICROSOFT WINDOWS

Computer:	**W10W (Standalone)**
Operating system:	**Windows 10 Pro (64bit)**
Audit date:	**2016-01-28 17:09**
Checklist:	**Audit Square - std. security/2016b**

Area	Check		Result *)
Basic tests	**BASE-01**	*OS version and updates*	Warning
	BASE-02	*Installed software*	Ok
	BASE-03	*Environment variables*	Ok
	BASE-04	*Other operating system settings*	Ok
System services	**SVCS-01**	*Basic configuration of system services*	Fail
	SVCS-02	*Drivers*	Warning
	SVCS-03	*Services and drivers access permissions*	Ok
	SVCS-04	*Service accounts*	Ok
	SVCS-05	*Other programs that run automatically*	Ok
Security policy	**SECP-01**	*Passwords and account locking policy*	Fail
	SECP-02	*Security settings*	Fail
	SECP-03	*Audit settings*	Fail
	SECP-04	*Parameters of log files*	Warning
	SECP-05	*Other security settings*	Fail
	SECP-06	*Privacy*	Warning
User accounts	**USER-01**	*System-wide privileges*	Fail
	USER-02	*Problematic active accounts*	Fail
	USER-03	*Local groups membership*	Fail
	USER-04	*Logon cache*	Ok
Access control	**ACLS-01**	*File system of local drives*	Ok
	ACLS-02	*File access permissions*	Ok
Network settings	**NETW-01**	*Global settings*	Fail
	NETW-02	*Problematic open TCP/UDP ports*	Warning
	NETW-03	*System server components configuration*	Ok
	NETW-04	*Shared resources*	Ok

*) You can get to detailed findings by clicking on the check result.

1 COMPUTER W10W

1.1 [INFO-xx] Assessment info

1.1.1 [INFO-01] Server/workstation

Brief description of the examined computer is shown in the table:

Computer name	W10W
Domain/workgroup membership	Workgroup (WORKGROUP)
Operating system version	10.0 (Windows 10 Pro)
CPU architecture, thread count	x86-64 x 1 (Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz)
Installed physical memory size	2.00 GB
HW classification	virtual (vmware)
OS root directory	C:\WINDOWS
OS install date	2016-01-14 12:08
Boot time	2016-01-28 16:28

[Computer W10W] [Top][Summary][Explanatory notes]

1.1.2 [INFO-02] Data collection

Data collection parameters are listed in the table below:

Collection date	2016-01-28 17:09
Account used	W10W\John Doe
Client version	2.7.4
Data processor version	1.1.3.1

[Computer W10W] [Top][Summary][Explanatory notes]

1.2 [BASE-xx] Basic tests

1.2.1 [BASE-01] OS version and updates

The check verifies the operating system version, installed service packs and hotfixes and settings of automatic updates service. If the version of the operating system is different from the given value, if the number of installed service pack is less than the specified value, if more than a specified time passed since the last hotfix installation, or if the configuration of automatic updates does not comply with the requirements, the overall result of a check is **FAIL**. Optional parameters allow to fine-tune the behavior of the check.

Check result: OK WITH WARNING.

The values to be verified are listed in the table below. Problematic values are marked in red:

Category	Parameter name	Value	Recommendation
Version	OS Version	WINDOWS 10 (10.0)	
	Service Pack	SP0	
Hotfixes and patches	Last hotfix installation date	2016-01-14	
Automatic Updates	Service status	Running/Manual (Trigger Start)	
	Updates configuration	Locally enabled (default setting)	
	Server redirection	--	☹ (local WSUS via encrypted connection (https))
	Status server redirection	--	☹ (local WSUS via encrypted

Category	Parameter name	Value	Recommendation
			connection (https))
	Delivery optimization	1 = subnet peering (locally)	☹ disable

[Computer W10W] [Top][Summary][Explanatory notes]

1.2.2 [BASE-02] Installed software

The installed software packages are checked against the set of rules. If any installed software does not comply with requirements, the overall result of the check is **FAIL**. Details of instances found are given in the results table.

Note: only the software installed by standard means and recorded in the system installation database is reported.

Check result: OK.

Problematic software packages must either be uninstalled or updated to the safe version, as indicated in the column with the recommendation.

Software	Producer	Version	Finding	Recommendation
Audit Square PRO Agent	AuditSquare.com	2.7.4	ok	
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161	ok	
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	Microsoft Corporation	9.0.30729.4148	ok	
VMware Tools	VMware, Inc.	9.9.2.2496486	ok	

[Computer W10W] [Top][Summary][Explanatory notes]

1.2.3 [BASE-03] Environment variables

The check verifies correctness of the settings of several important system environment variables, namely **COMSPEC**, **PATHEXT** and **PATH**. **COMSPEC** must refer to std. command interpreter (cmd.exe). **PATHEXT** must not contain non-default values for the given operating system. The most comprehensive is the testing of the **PATH** variable, which for the successful test outcome must not contain a directory writable by unprivileged users (exceptions can be specified using the check parameters if necessary).

Check result: OK.

These settings must be fixed manually directly on the server/workstation *(Control Panel - System - Advanced System Settings - Environment Variables)*. However, in the case of problematic entries in the **PATH**, the preferred solution is to fix directory permissions (removing the write permissions for unprivileged users and groups).Related link:Setting the PATH

Parameter	Value	Recommendation
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC	
ComSpec	C:\WINDOWS\system32\cmd.exe	
PATH	C:\WINDOWS\system32	
	C:\WINDOWS	
	C:\WINDOWS\system32\Wbem	
	C:\WINDOWS\system32\WindowsPowerShell\v1.0	

[Computer W10W] [Top][Summary][Explanatory notes]

1.2.4 [BASE-04] Other operating system settings

Check verifies the settings of several operating system parameters not included in other chapters. Audited settings include OS loader configuration, the OS response to fatal accidents, time synchronization and automatic login. Individual tests can optionally be turned off by the corresponding check arguments. The details of tests behavior can sometimes be further refined by check arguments as well.

Check result: OK.

The settings tested in this check must usually be adjusted manually directly on the computer without help of Group Policy. Details are beyond the scope of this report, please refer to the operating system manufacturer's documentation. Here only a quick hint on some topics:

- **OS loader** - *Control Panel - System - Advanced System Settings - Startup and Recovery*, or command line tools *(bootcfg, bcdedit)* (related link: DEP configuration);
- **Crash control** - *Control Panel - System - Advanced System Settings - Startup and Recovery* (related link: Crash control);
- **Automatic logon** - utility *netplwiz* (Windows Vista and higher), or direct modification of the registry, the key *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon* (related link: Disabling autologon).

Component	Parameter name	Value	Recommendation
OS clock	Time synchronization	Ok	
Winlogon	Automatic logon	Disabled	

[Computer W10W] [Top][Summary][Explanatory notes]

1.3 [SVCS-xx] System services

1.3.1 [SVCS-01] Basic configuration of system services

The check evaluates the configuration of system services, according to the specified set of rules. Following service attributes are verified: the current state of the service, its start mode, path to the binary image, image maker and image signer. With a set of custom rules blacklist-type checking can be performed (ban on the operation of certain services) as well as whitelist (allowing only the listed services) or requestlist (request the mandatory operation of certain services).

Check result: FAIL.

Security issues detected in this chapter may be fixed in different ways depending on the problem found: by removing or disabling the problematic services, adding them to the set of rules (whitelist), or changing the services' starting parameters. The latter could be performed locally (eg. by using mmc snap-in Services), but the use of Group Policy is recommended for efficiency reasons. GPO path to the settings is *Computer Configuration(/Policies)/Windows Settings/Security Settings/System Services*. However, caution is required when preparing the GPO; it should set only the service starting mode, but not service access permissions.

The table lists the system services with configuration or current state not matching the requirements:

Service	Status	Exe	Company	Signer	Recommendation
AJRouter (AllJoyn Router Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\AJRouter.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
ALG (Application Layer Gateway Service)	Stopped/Manual	C:\WINDOWS\system32\alg.exe	Microsoft Corporation	Microsoft Windows	
AppIDSvc (Application Identity)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\appidsvc.dll	Microsoft Corporation	Microsoft Windows	
Appinfo (Application Information)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\appinfo.dll	Microsoft Corporation	Microsoft Windows	
AppMgmt (Application Management)	Stopped/Manual	(svchost) C:\WINDOWS\system32\appmgmts.dll	Microsoft Corporation	Microsoft Windows	
AppReadiness (App Readiness)	Stopped/Manual	(svchost) C:\WINDOWS\system32\AppReadiness.dll	Microsoft Corporation	Microsoft Windows	
AppXSvc (AppX Deployment Service (AppXSVC))	Running/Manual	(svchost) C:\WINDOWS\system32\appxdeploymentserver.dll	Microsoft Corporation	Microsoft Windows	
AudioEndpointBuilder (Windows Audio Endpoint Builder)	Running/Auto	(svchost) C:\WINDOWS\system32\audioendpointbuild	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
		er.dll			
Audiosrv (Windows Audio)	Running/Auto	(svchost) C:\WINDOWS\system32\audiosrv.dll	Microsoft Corporation	Microsoft Windows	
AxInstSV (ActiveX Installer (AxInstSV))	Stopped/Manual	(svchost) C:\WINDOWS\system32\AxInstSv.dll	Microsoft Corporation	Microsoft Windows	
BDESVC (BitLocker Drive Encryption Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\bdesvc.dll	Microsoft Corporation	Microsoft Windows	
BFE (Base Filtering Engine)	Running/Auto	(svchost) C:\WINDOWS\system32\BFE.DLL	Microsoft Corporation	Microsoft Windows	
BITS (Background Intelligent Transfer Service)	Running/Auto (Delayed)	(svchost) C:\WINDOWS\system32\qmgr.dll	Microsoft Corporation	Microsoft Windows	
BrokerInfrastructure (Background Tasks Infrastructure Service)	Running/Auto	(svchost) C:\WINDOWS\system32\bisrv.dll	Microsoft Corporation	Microsoft Windows	
Browser (Computer Browser)	Stopped/Manual (Trigger Start, Trigger Stop)	(svchost) C:\WINDOWS\system32\browser.dll	Microsoft Corporation	Microsoft Windows	
BthHFSrv (Bluetooth Handsfree Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\BthHFSrv.dll	Microsoft Corporation	Microsoft Windows	
bthserv (Bluetooth Support Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\bthserv.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
CDPSvc (Connected Device Platform Service)	Stopped/Disabled	(svchost) C:\WINDOWS\system32\cdpsvc.dll	Microsoft Corporation	Microsoft Windows	
CertPropSvc (Certificate Propagation)	Stopped/Manual	(svchost) C:\WINDOWS\system32\certprop.dll	Microsoft Corporation	Microsoft Windows	
ClipSVC (Client License Service (ClipSVC))	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\ClipSVC.dll	Microsoft Corporation	Microsoft Windows	
COMSysApp (COM+ System Application)	Running/Manual	C:\WINDOWS\system32\dllhost.exe	Microsoft Corporation	Microsoft Windows	
CoreMessagingRegistrar (CoreMessaging)	Running/Auto	(svchost) C:\WINDOWS\system32\CoreMessaging.dll	Microsoft Corporation	Microsoft Windows	
CryptSvc (Cryptographic Services)	Running/Auto	(svchost) C:\WINDOWS\system32\cryptsvc.dll	Microsoft Corporation	Microsoft Windows	
CscService (Offline Files)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\cscsvc.dll	Microsoft Corporation	Microsoft Windows	
DcomLaunch (DCOM Server Process Launcher)	Running/Auto	(svchost) C:\WINDOWS\system32\rpcss.dll	Microsoft Corporation	Microsoft Windows	
DcpSvc (DataCollectionPublishingService)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\dcpsvc.dll	Microsoft Corporation	Microsoft Windows	
defragsvc (Optimize drives)	Running/Manual	(svchost) C:\WINDOWS\system32\defragsvc.dll	Microsoft Corporation	Microsoft Windows	
DeviceAssociationService (Device Association Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\das.dll	Microsoft Corporation	Microsoft Windows	
DeviceInstall (Device Install Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\umpnpmgr.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
DevQueryBroker (DevQuery Background Discovery Broker)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\DevQueryBroker.dll	Microsoft Corporation	Microsoft Windows	
Dhcp (DHCP Client)	Running/Auto	(svchost) C:\WINDOWS\system32\dhcpcore.dll	Microsoft Corporation	Microsoft Windows	
diagnosticshub.standardcollector.service (Microsoft (R) Diagnostics Hub Standard Collector Service)	Stopped/Manual	C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe	Microsoft Corporation	Microsoft Windows	
DiagTrack (Connected User Experiences and Telemetry)	Running/Auto	(svchost) C:\WINDOWS\system32\diagtrack.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
DmEnrollmentSvc (Device Management Enrollment Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\Windows.Internal.Management.dll	Microsoft Corporation	Microsoft Windows	
dmwappushservice (dmwappushsvc)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\dmwappushsvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
Dnscache (DNS Client)	Running/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\dnsrslvr.dll	Microsoft Corporation	Microsoft Windows	
DoSvc (Delivery Optimization)	Running/Auto (Delayed)	(svchost) C:\WINDOWS\system32\dosvc.dll	Microsoft Corporation	Microsoft Windows	
dot3svc (Wired AutoConfig)	Stopped/Manual	(svchost) C:\WINDOWS\system32\dot3svc.dll	Microsoft Corporation	Microsoft Windows	
DPS (Diagnostic Policy Service)	Running/Auto	(svchost) C:\WINDOWS\system32\dps.dll	Microsoft Corporation	Microsoft Windows	
DsmSvc (Device Setup Manager)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\DeviceSetupManager.dll	Microsoft Corporation	Microsoft Windows	
DsSvc (Data Sharing Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\dssvc.dll	Microsoft Corporation	Microsoft Windows	
Eaphost (Extensible Authentication Protocol)	Stopped/Manual	(svchost) C:\WINDOWS\system32\eapsvc.dll	Microsoft Corporation	Microsoft Windows	
EFS (Encrypting File System (EFS))	Stopped/Manual (Trigger Start)	C:\WINDOWS\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
embeddedmode (embeddedmode)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\embeddedmodesvc.dll	Microsoft Corporation	Microsoft Windows	
EntAppSvc (Enterprise App Management Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\EnterpriseAppMgmtSvc.dll	Microsoft Corporation	Microsoft Windows	
EventLog (Windows Event Log)	Running/Auto	(svchost) C:\WINDOWS\system32\wevtsvc.dll	Microsoft Corporation	Microsoft Windows	
EventSystem (COM+ Event System)	Running/Auto	(svchost) C:\WINDOWS\system32\es.dll	Microsoft Corporation	Microsoft Windows	
Fax (Fax)	Stopped/Manual	C:\WINDOWS\system32\FXSSVC.exe	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
fdPHost (Function	Running/Manual	(svchost)	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
Discovery Provider Host)		C:\WINDOWS\system32\fdPHost.dll			
FDResPub (Function Discovery Resource Publication)	Running/Manual	(svchost) C:\WINDOWS\system32\FDResPub.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
fhsvc (File History Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\fhsvc.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
FontCache (Windows Font Cache Service)	Running/Auto	(svchost) C:\WINDOWS\system32\FntCache.dll	Microsoft Corporation	Microsoft Windows	
gpsvc (Group Policy Client)	Running/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\gpsvc.dll	Microsoft Corporation	Microsoft Windows	
hidserv (Human Interface Device Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\hidserv.dll	Microsoft Corporation	Microsoft Windows	
HomeGroupListener (HomeGroup Listener)	Stopped/Manual	(svchost) C:\WINDOWS\system32\ListSvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
HomeGroupProvider (HomeGroup Provider)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\provsvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
icssvc (Windows Mobile Hotspot Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\tetheringservice.dll	Microsoft Corporation	Microsoft Windows	
IEEtwCollectorService (Internet Explorer ETW Collector Service)	Stopped/Manual	C:\WINDOWS\system32\IEEtwCollector.exe	Microsoft Corporation	Microsoft Windows	
IKEEXT (IKE and AuthIP IPsec Keying Modules)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\IKEEXT.DLL	Microsoft Corporation	Microsoft Windows	
iphlpsvc (IP Helper)	Running/Auto	(svchost) C:\WINDOWS\system32\iphlpsvc.dll	Microsoft Corporation	Microsoft Windows	
KeyIso (CNG Key Isolation)	Running/Manual (Trigger Start)	C:\WINDOWS\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
KtmRm (KtmRm for Distributed Transaction Coordinator)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\msdtckrm.dll	Microsoft Corporation	Microsoft Windows	
LanmanServer (Server)	Running/Auto	(svchost) C:\WINDOWS\system32\srvsvc.dll	Microsoft Corporation	Microsoft Windows	
LanmanWorkstation (Workstation)	Running/Auto	(svchost) C:\WINDOWS\system32\wkssvc.dll	Microsoft Corporation	Microsoft Windows	
lfsvc (Geolocation Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\lfsvc.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
LicenseManager (Windows License Manager Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\LicenseManagerSvc.dll	Microsoft Corporation	Microsoft Windows	
lltdsvc (Link-Layer Topology Discovery Mapper)	Stopped/Manual	(svchost) C:\WINDOWS\system32\lltdsvc.dll	Microsoft Corporation	Microsoft Windows	
lmhosts (TCP/IP NetBIOS Helper)	Running/Manual (Trigger Start, Trigger Stop)	(svchost) C:\WINDOWS\system32\lmhsvc.dll	Microsoft Corporation	Microsoft Windows	
LSM (Local Session Manager)	Running/Auto	(svchost) C:\WINDOWS\system32\lsm.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
MapsBroker (Downloaded Maps Manager)	Stopped/Auto (Delayed)	(svchost) C:\WINDOWS\system32\moshost.dll	Microsoft Corporation	Microsoft Windows	
MpsSvc (Windows Firewall)	Running/Auto	(svchost) C:\WINDOWS\system32\MPSSVC.dll	Microsoft Corporation	Microsoft Windows	
MSDTC (Distributed Transaction Coordinator)	Running/Manual	C:\WINDOWS\system32\msdtc.exe	Microsoft Corporation	Microsoft Windows	
MSiSCSI (Microsoft iSCSI Initiator Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\iscsiexe.dll	Microsoft Corporation	Microsoft Windows	
msiserver (Windows Installer)	Stopped/Manual	C:\WINDOWS\system32\msiexec.exe	Microsoft Corporation	Microsoft Windows	
NcaSvc (Network Connectivity Assistant)	Stopped/Manual (Trigger Start, Trigger Stop)	(svchost) C:\WINDOWS\system32\NcaSvc.dll	Microsoft Corporation	Microsoft Windows	
NcbService (Network Connection Broker)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\ncbservice.dll	Microsoft Corporation	Microsoft Windows	
NcdAutoSetup (Network Connected Devices Auto-Setup)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\NcdAutoSetup.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
Netlogon (Netlogon)	Stopped/Manual	C:\WINDOWS\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
Netman (Network Connections)	Stopped/Manual	(svchost) C:\WINDOWS\system32\netman.dll	Microsoft Corporation	Microsoft Windows	
netprofm (Network List Service)	Running/Manual	(svchost) C:\WINDOWS\system32\netprofmsvc.dll	Microsoft Corporation	Microsoft Windows	
NetSetupSvc (Network Setup Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\NetSetupSvc.dll	Microsoft Corporation	Microsoft Windows	
NetTcpPortSharing (Net.Tcp Port Sharing Service)	Stopped/Disabled	C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe	Microsoft Corporation	Microsoft Windows	
NgcCtnrSvc (Microsoft Passport Container)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\ngcctnrsvc.dll	Microsoft Corporation	Microsoft Windows	
NgcSvc (Microsoft Passport)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\ngcsvc.dll	Microsoft Corporation	Microsoft Windows	
NlaSvc (Network Location Awareness)	Running/Auto	(svchost) C:\WINDOWS\system32\nlasvc.dll	Microsoft Corporation	Microsoft Windows	
nsi (Network Store Interface Service)	Running/Auto	(svchost) C:\WINDOWS\system32\nsisvc.dll	Microsoft Corporation	Microsoft Windows	
p2pimsvc (Peer Networking Identity Manager)	Stopped/Manual	(svchost) C:\WINDOWS\system32\pnrpsvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
p2psvc (Peer Networking Grouping)	Stopped/Manual	(svchost) C:\WINDOWS\system32\p2psvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
PcaSvc (Program Compatibility Assistant Service)	Running/Auto	(svchost) C:\WINDOWS\system32\pcasvc.dll	Microsoft Corporation	Microsoft Windows	
PeerDistSvc (BranchCache)	Stopped/Manual	(svchost) C:\WINDOWS\system32\peerdistsvc.dll	Microsoft Corporation	Microsoft Windows	
PerfHost (Performance Counter	Stopped/Manual	C:\WINDOWS\SysWOW64\perfhost.exe	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
DLL Host)					
PhoneSvc (Phone Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\PhoneService.dll	Microsoft Corporation	Microsoft Windows	
pla (Performance Logs & Alerts)	Stopped/Manual	(svchost) C:\WINDOWS\system32\pla.dll	Microsoft Corporation	Microsoft Windows	
PlugPlay (Plug and Play)	Running/Manual	(svchost) C:\WINDOWS\system32\umpnpmgr.dll	Microsoft Corporation	Microsoft Windows	
PNRPAutoReg (PNRP Machine Name Publication Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\pnrpauto.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
PNRPsvc (Peer Name Resolution Protocol)	Stopped/Manual	(svchost) C:\WINDOWS\system32\pnrpsvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
PolicyAgent (IPsec Policy Agent)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\IPSECSVC.DLL	Microsoft Corporation	Microsoft Windows	
Power (Power)	Running/Auto	(svchost) C:\WINDOWS\system32\umpo.dll	Microsoft Corporation	Microsoft Windows	
PrintNotify (Printer Extensions and Notifications)	Stopped/Manual	(svchost) C:\WINDOWS\system32\spool\drivers\x64\3\PrintConfig.dll	Microsoft Corporation	Microsoft Windows	
ProfSvc (User Profile Service)	Running/Auto	(svchost) C:\WINDOWS\system32\profsvc.dll	Microsoft Corporation	Microsoft Windows	
QWAVE (Quality Windows Audio Video Experience)	Stopped/Manual	(svchost) C:\WINDOWS\system32\qwave.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
RasAuto (Remote Access Auto Connection Manager)	Stopped/Manual	(svchost) C:\WINDOWS\system32\rasauto.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
RasMan (Remote Access Connection Manager)	Stopped/Manual	(svchost) C:\WINDOWS\system32\rasmans.dll	Microsoft Corporation	Microsoft Windows	
RemoteAccess (Routing and Remote Access)	Stopped/Disabled	(svchost) C:\WINDOWS\system32\mprdim.dll	Microsoft Corporation	Microsoft Windows	
RemoteRegistry (Remote Registry)	Stopped/Disabled	(svchost) C:\WINDOWS\system32\regsvc.dll	Microsoft Corporation	Microsoft Windows	
RetailDemo (Retail Demo Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\RDXService.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
RpcEptMapper (RPC Endpoint Mapper)	Running/Auto	(svchost) C:\WINDOWS\system32\RpcEpMap.dll	Microsoft Corporation	Microsoft Windows	
RpcLocator (Remote Procedure Call (RPC) Locator)	Stopped/Manual	C:\WINDOWS\system32\Locator.exe	Microsoft Corporation	Microsoft Windows	
RpcSs (Remote Procedure Call (RPC))	Running/Auto	(svchost) C:\WINDOWS\system32\rpcss.dll	Microsoft Corporation	Microsoft Windows	
SamSs (Security Accounts Manager)	Running/Auto	C:\WINDOWS\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
SCardSvr (Smart Card)	Stopped/Disabled	(svchost) C:\WINDOWS\system32\SCardSvr.dll	Microsoft Corporation	Microsoft Windows	
ScDeviceEnum (Smart Card Device Enumeration Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\scdeviceenum.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
Schedule (Task Scheduler)	Running/Auto	(svchost) C:\WINDOWS\system32\schedsvc.dll	Microsoft Corporation	Microsoft Windows	
SCPolicySvc (Smart Card Removal Policy)	Stopped/Manual	(svchost) C:\WINDOWS\system32\certprop.dll	Microsoft Corporation	Microsoft Windows	
SDRSVC (Windows Backup)	Stopped/Manual	(svchost) C:\WINDOWS\system32\sdrsvc.dll	Microsoft Corporation	Microsoft Windows	
seclogon (Secondary Logon)	Stopped/Manual	(svchost) C:\WINDOWS\system32\seclogon.dll	Microsoft Corporation	Microsoft Windows	
SENS (System Event Notification Service)	Running/Auto	(svchost) C:\WINDOWS\system32\Sens.dll	Microsoft Corporation	Microsoft Windows	
SensorDataService (Sensor Data Service)	Stopped/Manual (Trigger Start)	C:\WINDOWS\system32\SensorDataService.exe	Microsoft Corporation	Microsoft Windows	
SensorService (Sensor Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\SensorService.dll	Microsoft Corporation	Microsoft Windows	
SensrSvc (Sensor Monitoring Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\sensrsvc.dll	Microsoft Corporation	Microsoft Windows	
SessionEnv (Remote Desktop Configuration)	Stopped/Manual	(svchost) C:\WINDOWS\system32\SessEnv.dll	Microsoft Corporation	Microsoft Windows	
SharedAccess (Internet Connection Sharing (ICS))	Stopped/Manual	(svchost) C:\WINDOWS\system32\ipnathlp.dll	Microsoft Corporation	Microsoft Windows	
ShellHWDetection (Shell Hardware Detection)	Running/Auto	(svchost) C:\WINDOWS\system32\shsvcs.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
smphost (Microsoft Storage Spaces SMP)	Stopped/Manual	(svchost) C:\WINDOWS\system32\smphost.dll	Microsoft Corporation	Microsoft Windows	
SmsRouter (Microsoft Windows SMS Router Service.)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\SmsRouterSvc.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
SNMPTRAP (SNMP Trap)	Stopped/Manual	C:\WINDOWS\system32\snmptrap.exe	Microsoft Corporation	Microsoft Windows	
Spooler (Print Spooler)	Running/Auto	C:\WINDOWS\system32\spoolsv.exe	Microsoft Corporation	Microsoft Windows	
sppsvc (Software Protection)	Stopped/Auto (Delayed, Trigger Start)	C:\WINDOWS\system32\sppsvc.exe	Microsoft Corporation	Microsoft Windows	
SSDPSRV (SSDP Discovery)	Running/Manual	(svchost) C:\WINDOWS\system32\ssdpsrv.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
SstpSvc (Secure Socket Tunneling Protocol Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\sstpsvc.dll	Microsoft Corporation	Microsoft Windows	
StateRepository (State Repository Service)	Running/Manual	(svchost) C:\WINDOWS\system32\Windows.StateRepository.dll	Microsoft Corporation	Microsoft Windows	
stisvc (Windows Image Acquisition (WIA))	Stopped/Manual	(svchost) C:\WINDOWS\system32\wiaservc.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
StorSvc (Storage Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\StorSvc.dll	Microsoft Corporation	Microsoft Windows	
svsvc (Spot Verifier)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
		32\svsvc.dll			
swprv (Microsoft Software Shadow Copy Provider)	Stopped/Manual	(svchost) C:\WINDOWS\system32\swprv.dll	Microsoft Corporation	Microsoft Windows	
SysMain (Superfetch)	Running/Auto	(svchost) C:\WINDOWS\system32\sysmain.dll	Microsoft Corporation	Microsoft Windows	
SystemEventsBroker (System Events Broker)	Running/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\systemeventsbrokerserver.dll	Microsoft Corporation	Microsoft Windows	
TabletInputService (Touch Keyboard and Handwriting Panel Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\TabSvc.dll	Microsoft Corporation	Microsoft Windows	
TapiSrv (Telephony)	Stopped/Manual	(svchost) C:\WINDOWS\system32\tapisrv.dll	Microsoft Corporation	Microsoft Windows	
TermService (Remote Desktop Services)	Stopped/Manual	(svchost) C:\WINDOWS\system32\termsrv.dll	Microsoft Corporation	Microsoft Windows	
Themes (Themes)	Running/Auto	(svchost) C:\WINDOWS\system32\themeservice.dll	Microsoft Corporation	Microsoft Windows	
TieringEngineService (Storage Tiers Management)	Stopped/Manual	C:\WINDOWS\system32\TieringEngineService.exe	Microsoft Corporation	Microsoft Windows	
tiledatamodelsvc (Tile Data model server)	Running/Auto	(svchost) C:\WINDOWS\system32\tileobjserver.dll	Microsoft Corporation	Microsoft Windows	
TimeBroker (Time Broker)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\timebrokerserver.dll	Microsoft Corporation	Microsoft Windows	
TPAutoConnSvc (TP AutoConnect Service)	Running/Manual	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe	Cortado AG	Cortado AG	
TPVCGateway (TP VC Gateway Service)	Stopped/Manual	C:\Program Files\VMware\VMware Tools\TPVCGateway.exe	Cortado AG	Cortado AG	
TrkWks (Distributed Link Tracking Client)	Running/Auto	(svchost) C:\WINDOWS\system32\trkwks.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
TrustedInstaller (Windows Modules Installer)	Stopped/Auto	C:\WINDOWS\servicing\TrustedInstaller.exe	Microsoft Corporation	Microsoft Windows	
tzautoupdate (Auto Time Zone Updater)	Stopped/Disabled	(svchost) C:\WINDOWS\system32\tzautoupdate.dll	Microsoft Corporation	Microsoft Windows	
UI0Detect (Interactive Services Detection)	Stopped/Manual	C:\WINDOWS\system32\UI0Detect.exe	Microsoft Corporation	Microsoft Windows	
UmRdpService (Remote Desktop Services UserMode Port Redirector)	Stopped/Manual	(svchost) C:\WINDOWS\system32\umrdp.dll	Microsoft Corporation	Microsoft Windows	
upnphost (UPnP Device Host)	Stopped/Manual	(svchost) C:\WINDOWS\system32\upnphost.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
UserManager (User Manager)	Running/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\usermgr.dll	Microsoft Corporation	Microsoft Windows	
UsoSvc (Update	Stopped/Manual	(svchost)	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
Orchestrator Service)		C:\WINDOWS\system32\usocore.dll			
VaultSvc (Credential Manager)	Running/Manual	C:\WINDOWS\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
vds (Virtual Disk)	Stopped/Manual	C:\WINDOWS\system32\vds.exe	Microsoft Corporation	Microsoft Windows	
vmicguestinterface (Hyper-V Guest Service Interface)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicheartbeat (Hyper-V Heartbeat Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmickvpexchange (Hyper-V Data Exchange Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicrdv (Hyper-V Remote Desktop Virtualization Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicshutdown (Hyper-V Guest Shutdown Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmictimesync (Hyper-V Time Synchronization Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicvmsession (Hyper-V VM Session Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicvss (Hyper-V Volume Shadow Copy Requestor)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
VMTools (VMware Tools)	Running/Auto	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	VMware, Inc.	VMware, Inc.	
vmvss (VMware Snapshot Provider)	Stopped/Manual	C:\WINDOWS\system32\dllhost.exe	Microsoft Corporation	Microsoft Windows	
VSS (Volume Shadow Copy)	Stopped/Manual	C:\WINDOWS\system32\VSSVC.exe	Microsoft Corporation	Microsoft Windows	
W32Time (Windows Time)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\w32time.dll	Microsoft Corporation	Microsoft Windows	
WalletService (WalletService)	Stopped/Manual	(svchost) C:\WINDOWS\system32\WalletService.dll	Microsoft Corporation	Microsoft Windows	
wbengine (Block Level Backup Engine Service)	Stopped/Manual	C:\WINDOWS\system32\wbengine.exe	Microsoft Corporation	Microsoft Windows	
WbioSrvc (Windows Biometric Service)	Stopped/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\wbiosrvc.dll	Microsoft Corporation	Microsoft Windows	
Wcmsvc (Windows Connection Manager)	Running/Auto (Trigger Start)	(svchost) C:\WINDOWS\system32\wcmsvc.dll	Microsoft Corporation	Microsoft Windows	
wcncsvc (Windows Connect Now - Config Registrar)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wcncsvc.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
WcsPlugInService (Windows Color System)	Stopped/Manual	(svchost) C:\WINDOWS\system32\WcsPlugInService.dll	Microsoft Corporation	Microsoft Windows	
WdiServiceHost (Diagnostic Service Host)	Running/Manual	(svchost) C:\WINDOWS\system32\wdi.dll	Microsoft Corporation	Microsoft Windows	
WdiSystemHost	Running/Manual	(svchost)	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
(Diagnostic System Host)		C:\WINDOWS\system32\wdi.dll			
WdNisSvc (Windows Defender Network Inspection Service)	Running/Manual	C:\Program Files\Windows Defender\NisSrv.exe	Microsoft Corporation	Microsoft Windows	
WebClient (WebClient)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\WebClnt.dll	Microsoft Corporation	Microsoft Windows	
Wecsvc (Windows Event Collector)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wecsvc.dll	Microsoft Corporation	Microsoft Windows	
WEPHOSTSVC (Windows Encryption Provider Host Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\wephostsvc.dll	Microsoft Corporation	Microsoft Windows	
wercplsupport (Problem Reports and Solutions Control Panel Support)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wercplsupport.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
WerSvc (Windows Error Reporting Service)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\wersvc.dll	Microsoft Corporation	Microsoft Windows	
WiaRpc (Still Image Acquisition Events)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wiarpc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
WinDefend (Windows Defender Service)	Running/Auto	C:\Program Files\Windows Defender\MsMpEng.exe	Microsoft Corporation	Microsoft Windows	
WinHttpAutoProxySvc (WinHTTP Web Proxy Auto-Discovery Service)	Running/Manual	(svchost) C:\WINDOWS\system32\winhttp.dll	Microsoft Corporation	Microsoft Windows	
Winmgmt (Windows Management Instrumentation)	Running/Auto	(svchost) C:\WINDOWS\system32\wbem\WMIsvc.dll	Microsoft Corporation	Microsoft Windows	
WinRM (Windows Remote Management (WS-Management))	Stopped/Manual	(svchost) C:\WINDOWS\system32\WsmSvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
WlanSvc (WLAN AutoConfig)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wlansvc.dll	Microsoft Corporation	Microsoft Windows	
wlidsvc (Microsoft Account Sign-in Assistant)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\wlidsvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
wmiApSrv (WMI Performance Adapter)	Stopped/Manual	C:\WINDOWS\system32\wbem\WmiApSrv.exe	Microsoft Corporation	Microsoft Windows	
WMPNetworkSvc (Windows Media Player Network Sharing Service)	Stopped/Manual	C:\Program Files\Windows Media Player\wmpnetwk.exe	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
workfolderssvc (Work Folders)	Stopped/Manual	(svchost) C:\WINDOWS\system32\workfolderssvc.dll	Microsoft Corporation	Microsoft Windows	
WPDBusEnum (Portable Device Enumerator Service)	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\wpdbusenum.dll	Microsoft Corporation	Microsoft Windows	
WpnService (Windows Push Notifications Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\WpnService.dll	Microsoft Corporation	Microsoft Windows	
wscsvc (Security Center)	Running/Auto (Delayed)	(svchost) C:\WINDOWS\system32\wscsvc.dll	Microsoft Corporation	Microsoft Windows	
WSearch (Windows Search)	Running/Auto (Delayed)	C:\WINDOWS\system32\SearchIndexer.exe	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
WSService (Windows Store Service (WSService))	Stopped/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\WSService.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
wuauserv (Windows Update)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\wuaueng.dll	Microsoft Corporation	Microsoft Windows	
wudfsvc (Windows Driver Foundation - User-mode Driver Framework)	Running/Manual (Trigger Start)	(svchost) C:\WINDOWS\system32\WUDFSvc.dll	Microsoft Corporation	Microsoft Windows	
WwanSvc (WWAN AutoConfig)	Stopped/Manual	(svchost) C:\WINDOWS\system32\wwansvc.dll	Microsoft Corporation	Microsoft Windows	
XblAuthManager (Xbox Live Auth Manager)	Stopped/Manual	(svchost) C:\WINDOWS\system32\XblAuthManager.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
XblGameSave (Xbox Live Game Save)	Stopped/Manual	(svchost) C:\WINDOWS\system32\XblGameSave.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
XboxNetApiSvc (Xbox Live Networking Service)	Stopped/Manual	(svchost) C:\WINDOWS\system32\XboxNetApiSvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)

[Computer W10W] [Top][Summary][Explanatory notes]

1.3.2 [SVCS-02] Drivers

The check evaluates the configuration of system drivers, according to the specified set of rules. Following driver attributes are verified: the current state of the driver, its start mode, path to the binary image, image maker and image signer. With a set of custom rules blacklist-type checking can be performed (ban on the operation of certain drivers) as well as whitelist (allowing only the listed drivers) or requestlist (request the mandatory operation of certain drivers).

Check result: OK WITH WARNING.

Fixing of security issues detected in this chapter used to be rather problematic, the driver usually can only be disabled or completely removed, or perhaps updated to newer version.

The table lists the system drivers with configuration or current state not matching the requirements:

Driver	Status	Exe	Company	Signer	Recommendation
1394ohci (1394 OHCI Compliant Host Controller)	Stopped/Manual	C:\WINDOWS\system32\drivers\1394ohci.sys	Microsoft Corporation	Microsoft Windows	
3ware (3ware)	Stopped/Manual	C:\WINDOWS\system32\drivers\3ware.sys	LSI	Microsoft Windows	
ACPI (Microsoft ACPI Driver)	Running/Boot	C:\WINDOWS\system32\drivers\acpi.sys	Microsoft Corporation	Microsoft Windows	
acpiex (Microsoft ACPIEx Driver)	Running/Boot	C:\WINDOWS\system32\drivers\acpiex.sys	Microsoft Corporation	Microsoft Windows	
acpipagr (ACPI Processor Aggregator Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\acpipagr.sys	Microsoft Corporation	Microsoft Windows	
AcpiPmi (ACPI Power Meter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\acpipmi.sys	Microsoft Corporation	Microsoft Windows	
acpitime (ACPI Wake Alarm Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\acpitime.sys	Microsoft Corporation	Microsoft Windows	
ADP80XX (ADP80XX)	Stopped/Manual	C:\WINDOWS\system32\drivers\adp80xx.sys	PMC-Sierra	Microsoft Windows	
AFD (Ancillary Function Driver for Winsock)	Running/System	C:\WINDOWS\system32\drivers\afd.sys	Microsoft Corporation	Microsoft Windows	
agp440 (Intel AGP	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Bus Filter)		32\drivers\AGP440.sys			
ahcache (Application Compatibility Cache)	Running/System	C:\WINDOWS\system32\drivers\ahcache.sys	Microsoft Corporation	Microsoft Windows	
AmdK8 (AMD K8 Processor Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\amdk8.sys	Microsoft Corporation	Microsoft Windows	
AmdPPM (AMD Processor Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\amdppm.sys	Microsoft Corporation	Microsoft Windows	
amdsata (amdsata)	Stopped/Manual	C:\WINDOWS\system32\drivers\amdsata.sys	Advanced Micro Devices	Microsoft Windows	
amdsbs (amdsbs)	Stopped/Manual	C:\WINDOWS\system32\drivers\amdsbs.sys	AMD Technologies Inc.	Microsoft Windows	
amdxata (amdxata)	Stopped/Manual	C:\WINDOWS\system32\drivers\amdxata.sys	Advanced Micro Devices	Microsoft Windows	
AppID (AppID Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\appid.sys	Microsoft Corporation	Microsoft Windows	
arcsas (Adaptec SAS/SATA-II RAID Storport's Miniport Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\arcsas.sys	PMC-Sierra, Inc.	Microsoft Windows	
AsyncMac (RAS Asynchronous Media Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\asyncmac.sys	Microsoft Corporation	Microsoft Windows	
atapi (IDE Channel)	Running/Boot	C:\WINDOWS\system32\drivers\atapi.sys	Microsoft Corporation	Microsoft Windows	
b06bdrv (Broadcom NetXtreme II VBD)	Stopped/Manual	C:\WINDOWS\system32\drivers\bxvbda.sys	Broadcom Corporation	Microsoft Windows	
BasicDisplay (BasicDisplay)	Running/System	C:\WINDOWS\system32\drivers\BasicDisplay.sys	Microsoft Corporation	Microsoft Windows	
BasicRender (BasicRender)	Running/System	C:\WINDOWS\system32\drivers\BasicRender.sys	Microsoft Corporation	Microsoft Windows	
bcmfn (bcmfn Service)	Stopped/Manual	C:\WINDOWS\system32\drivers\bcmfn.sys	Windows (R) Win 7 DDK provider	Microsoft Windows	
bcmfn2 (bcmfn2 Service)	Stopped/Manual	C:\WINDOWS\system32\drivers\bcmfn2.sys	Windows (R) Win 7 DDK provider	Microsoft Windows	
bowser (Browser Support Driver)	Running/Manual	C:\WINDOWS\system32\drivers\bowser.sys	Microsoft Corporation	Microsoft Windows	
BthAvrcpTg (Bluetooth Audio/Video Remote Control HID)	Stopped/Manual	C:\WINDOWS\system32\drivers\BthAvrcpTg.sys	Microsoft Corporation	Microsoft Windows	
BthHFEnum (Bluetooth Hands-Free Audio and Call Control HID Enumerator)	Stopped/Manual	C:\WINDOWS\system32\drivers\bthhfenum.sys	Microsoft Corporation	Microsoft Windows	
bthhfhid (Bluetooth Hands-Free Call Control HID)	Stopped/Manual	C:\WINDOWS\system32\drivers\BthhfHid.sys	Microsoft Corporation	Microsoft Windows	
BTHMODEM (Bluetooth Modem Communications Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\bthmodem.sys	Microsoft Corporation	Microsoft Windows	
buttonconverter (Service for Portable Device Control devices)	Stopped/Manual	C:\WINDOWS\system32\drivers\buttonconverter.sys	Microsoft Corporation	Microsoft Windows	
CapImg (HID driver	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
for CapImg touch screen)		32\drivers\capimg.sys			
cdfs (CD/DVD File System Reader)	Stopped/Disabled	C:\WINDOWS\system32\drivers\cdfs.sys	Microsoft Corporation	Microsoft Windows	
cdrom (CD-ROM Driver)	Running/System	C:\WINDOWS\system32\drivers\cdrom.sys	Microsoft Corporation	Microsoft Windows	
circlass (Consumer IR Devices)	Stopped/Manual	C:\WINDOWS\system32\drivers\circlass.sys	Microsoft Corporation	Microsoft Windows	
CLFS (Common Log (CLFS))	Running/Boot	C:\WINDOWS\system32\drivers\clfs.sys	Microsoft Corporation	Microsoft Windows	
CmBatt (Microsoft ACPI Control Method Battery Driver)	Running/Manual	C:\WINDOWS\system32\drivers\CmBatt.sys	Microsoft Corporation	Microsoft Windows	
CNG (CNG)	Running/Boot	C:\WINDOWS\system32\drivers\cng.sys	Microsoft Corporation	Microsoft Windows	
cnghwassist (CNG Hardware Assist algorithm provider)	Stopped/Disabled	C:\WINDOWS\system32\drivers\cnghwassist.sys	Microsoft Corporation	Microsoft Windows	
CompositeBus (Composite Bus Enumerator Driver)	Running/Manual	C:\WINDOWS\system32\DriverStore\FileRepository\compositebus.inf_amd64_912dfdedc3d2f520\CompositeBus.sys	Microsoft Corporation	Microsoft Windows	
condrv (Console Driver)	Running/Manual	C:\WINDOWS\system32\drivers\condrv.sys	Microsoft Corporation	Microsoft Windows	
CSC (Offline Files Driver)	Running/System	C:\WINDOWS\system32\drivers\csc.sys	Microsoft Corporation	Microsoft Windows	
dam (Desktop Activity Moderator Driver)	Stopped/System	C:\WINDOWS\system32\drivers\dam.sys	Microsoft Corporation	Microsoft Windows	
Dfsc (DFS Namespace Client Driver)	Running/System	C:\WINDOWS\system32\drivers\dfsc.sys	Microsoft Corporation	Microsoft Windows	
disk (Disk Driver)	Running/Boot	C:\WINDOWS\system32\drivers\disk.sys	Microsoft Corporation	Microsoft Windows	
dmvsc (dmvsc)	Stopped/Manual	C:\WINDOWS\system32\drivers\dmvsc.sys	Microsoft Corporation	Microsoft Windows	
drmkaud (Microsoft Trusted Audio Drivers)	Stopped/Manual	C:\WINDOWS\system32\drivers\drmkaud.sys	Microsoft Corporation	Microsoft Windows	
DXGKrnl (LDDM Graphics Subsystem)	Running/Manual	C:\WINDOWS\system32\drivers\dxgkrnl.sys	Microsoft Corporation	Microsoft Windows	
e1iexpress (Intel(R) PRO/1000 PCI Express Network Connection Driver I)	Running/Manual	C:\WINDOWS\system32\drivers\e1i63x64.sys	Intel Corporation	Microsoft Windows	
ebdrv (QLogic 10 Gigabit Ethernet Adapter VBD)	Stopped/Manual	C:\WINDOWS\system32\drivers\evbda.sys	QLogic Corporation	Microsoft Windows	
EhStorClass (Enhanced Storage Filter Driver)	Running/Boot	C:\WINDOWS\system32\drivers\EhStorClass.sys	Microsoft Corporation	Microsoft Windows	
EhStorTcgDrv (Microsoft driver for storage devices supporting IEEE 1667 and TCG protocols)	Stopped/Manual	C:\WINDOWS\system32\drivers\EhStorTcgDrv.sys	Microsoft Corporation	Microsoft Windows	
ErrDev (Microsoft Hardware Error Device Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\errdev.sys	Microsoft Corporation	Microsoft Windows	
fdc (Floppy Disk Controller Driver)	Running/Manual	C:\WINDOWS\system32\drivers\fdc.sys	Microsoft Corporation	Microsoft Windows	
FileCrypt (FileCrypt)	Running/System	C:\WINDOWS\system32\drivers\filecrypt.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
FileInfo (File Information FS MiniFilter)	Running/Boot	C:\WINDOWS\system32\drivers\fileinfo.sys	Microsoft Corporation	Microsoft Windows	
Filetrace (Filetrace)	Stopped/Manual	C:\WINDOWS\system32\drivers\filetrace.sys	Microsoft Corporation	Microsoft Windows	
flpydisk (Floppy Disk Driver)	Running/Manual	C:\WINDOWS\system32\drivers\flpydisk.sys	Microsoft Corporation	Microsoft Windows	
FltMgr (FltMgr)	Running/Boot	C:\WINDOWS\system32\drivers\fltMgr.sys	Microsoft Corporation	Microsoft Windows	
FsDepends (File System Dependency Minifilter)	Stopped/Manual	C:\WINDOWS\system32\drivers\FsDepends.sys	Microsoft Corporation	Microsoft Windows	
fvevol (BitLocker Drive Encryption Filter Driver)	Running/Boot	C:\WINDOWS\system32\drivers\fvevol.sys	Microsoft Corporation	Microsoft Windows	
gagp30kx (Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms)	Stopped/Manual	C:\WINDOWS\system32\drivers\GAGP30KX.SYS	Microsoft Corporation	Microsoft Windows	
gencounter (Microsoft Hyper-V Generation Counter)	Running/Manual	C:\WINDOWS\system32\drivers\vmgencounter.sys	Microsoft Corporation	Microsoft Windows	
genericusbfn (Generic USB Function Class)	Stopped/Manual	C:\WINDOWS\system32\drivers\genericusbfn.sys	Microsoft Corporation	Microsoft Windows	
GPIOClx0101 (Microsoft GPIO Class Extension Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\msgpioclx.sys	Microsoft Corporation	Microsoft Windows	
GpuEnergyDrv (GPU Energy Driver)	Running/System	C:\WINDOWS\system32\drivers\gpuenergydrv.sys	Microsoft Corporation	Microsoft Windows	
HdAudAddService (Microsoft 1.1 UAA Function Driver for High Definition Audio Service)	Running/Manual	C:\WINDOWS\system32\drivers\HdAudio.sys	Microsoft Corporation	Microsoft Windows	
HDAudBus (Microsoft UAA Bus Driver for High Definition Audio)	Running/Manual	C:\WINDOWS\system32\drivers\hdaudbus.sys	Microsoft Corporation	Microsoft Windows	
HidBatt (HID UPS Battery Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\hidbatt.sys	Microsoft Corporation	Microsoft Windows	
HidBth (Microsoft Bluetooth HID Miniport)	Stopped/Manual	C:\WINDOWS\system32\drivers\hidbth.sys	Microsoft Corporation	Microsoft Windows	
hidi2c (Microsoft I2C HID Miniport Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\hidi2c.sys	Microsoft Corporation	Microsoft Windows	
hidinterrupt (Common Driver for HID Buttons implemented with interrupts)	Stopped/Manual	C:\WINDOWS\system32\drivers\hidinterrupt.sys	Microsoft Corporation	Microsoft Windows	
HidIr (Microsoft Infrared HID Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\hidir.sys	Microsoft Corporation	Microsoft Windows	
HidUsb (Microsoft HID Class Driver)	Running/Manual	C:\WINDOWS\system32\drivers\hidusb.sys	Microsoft Corporation	Microsoft Windows	
HpSAMD (HpSAMD)	Stopped/Manual	C:\WINDOWS\system32\drivers\HpSAMD.sys	Hewlett-Packard Company	Microsoft Windows	
HTTP (HTTP Service)	Running/Manual	C:\WINDOWS\system32\drivers\http.sys	Microsoft Corporation	Microsoft Windows	
hwpolicy (Hardware Policy Driver)	Stopped/Boot	C:\WINDOWS\system32\drivers\hwpolicy.sys	Microsoft Corporation	Microsoft Windows	
hyperkbd (hyperkbd)	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
		32\drivers\hyperkbd.sys			
i8042prt (PS/2 Keyboard and Mouse Port Driver)	Running/Manual	C:\WINDOWS\system32\drivers\i8042prt.sys	Microsoft Corporation	Microsoft Windows	
iai2c (Intel(R) Serial IO I2C Host Controller)	Stopped/Manual	C:\WINDOWS\system32\drivers\iai2c.sys	Intel(R) Corporation	Microsoft Windows	
iaLPSS2i_I2C (Intel(R) Serial IO I2C Driver v2)	Stopped/Manual	C:\WINDOWS\system32\drivers\iaLPSS2i_I2C.sys	Intel Corporation	Microsoft Windows	
iaLPSSi_GPIO (Intel(R) Serial IO GPIO Controller Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\iaLPSSi_GPIO.sys	Intel Corporation	Microsoft Windows	
iaLPSSi_I2C (Intel(R) Serial IO I2C Controller Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\iaLPSSi_I2C.sys	Intel Corporation	Microsoft Windows	
iaStorAV (Intel(R) SATA RAID Controller Windows)	Stopped/Manual	C:\WINDOWS\system32\drivers\iaStorAV.sys	Intel Corporation	Microsoft Windows	
iaStorV (Intel RAID Controller Windows 7)	Stopped/Manual	C:\WINDOWS\system32\drivers\iaStorV.sys	Intel Corporation	Microsoft Windows	
ibbus (Mellanox InfiniBand Bus/AL (Filter Driver))	Stopped/Manual	C:\WINDOWS\system32\drivers\ibbus.sys	Mellanox	Microsoft Windows	
intelide (intelide)	Running/Boot	C:\WINDOWS\system32\drivers\intelide.sys	Microsoft Corporation	Microsoft Windows	
intelpep (Intel(R) Power Engine Plug-in Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\intelpep.sys	Microsoft Corporation	Microsoft Windows	
intelppm (Intel Processor Driver)	Running/Manual	C:\WINDOWS\system32\drivers\intelppm.sys	Microsoft Corporation	Microsoft Windows	
IoQos (IoQos)	Stopped/Manual	C:\WINDOWS\system32\drivers\ioqos.sys	Microsoft Corporation	Microsoft Windows	
IpFilterDriver (IP Traffic Filter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\ipfltdrv.sys	Microsoft Corporation	Microsoft Windows	
IPMIDRV (IPMIDRV)	Stopped/Manual	C:\WINDOWS\system32\drivers\IPMIDrv.sys	Microsoft Corporation	Microsoft Windows	
IPNAT (IP Network Address Translator)	Stopped/Manual	C:\WINDOWS\system32\drivers\ipnat.sys	Microsoft Corporation	Microsoft Windows	
IRENUM (IR Bus Enumerator)	Stopped/Manual	C:\WINDOWS\system32\drivers\irenum.sys	Microsoft Corporation	Microsoft Windows	
isapnp (isapnp)	Stopped/Manual	C:\WINDOWS\system32\drivers\isapnp.sys	Microsoft Corporation	Microsoft Windows	
iScsiPrt (iScsiPort Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\msiscsi.sys	Microsoft Corporation	Microsoft Windows	
kbdclass (Keyboard Class Driver)	Running/Manual	C:\WINDOWS\system32\drivers\kbdclass.sys	Microsoft Corporation	Microsoft Windows	
kbdhid (Keyboard HID Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\kbdhid.sys	Microsoft Corporation	Microsoft Windows	
kdnic (Microsoft Kernel Debug Network Miniport (NDIS 6.20))	Running/Manual	C:\WINDOWS\system32\drivers\kdnic.sys	Microsoft Corporation	Microsoft Windows	
KSecDD (KSecDD)	Running/Boot	C:\WINDOWS\system32\drivers\ksecdd.sys	Microsoft Corporation	Microsoft Windows	
KSecPkg (KSecPkg)	Running/Boot	C:\WINDOWS\system32\drivers\ksecpkg.sys	Microsoft Corporation	Microsoft Windows	
ksthunk (Kernel	Running/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Streaming Thunks)		32\drivers\ksthunk.sys			
lltdio (Link-Layer Topology Discovery Mapper I/O Driver)	Running/Auto	C:\WINDOWS\system32\drivers\lltdio.sys	Microsoft Corporation	Microsoft Windows	
LSI_SAS (LSI_SAS)	Running/Boot	C:\WINDOWS\system32\drivers\lsi_sas.sys	LSI Corporation	Microsoft Windows	
LSI_SAS2i (LSI_SAS2i)	Stopped/Manual	C:\WINDOWS\system32\drivers\lsi_sas2i.sys	LSI Corporation	Microsoft Windows	
LSI_SAS3i (LSI_SAS3i)	Stopped/Manual	C:\WINDOWS\system32\drivers\lsi_sas3i.sys	Avago Technologies	Microsoft Windows	
LSI_SSS (LSI_SSS)	Stopped/Manual	C:\WINDOWS\system32\drivers\lsi_sss.sys	LSI Corporation	Microsoft Windows	
luafv (UAC File Virtualization)	Running/Auto	C:\WINDOWS\system32\drivers\luafv.sys	Microsoft Corporation	Microsoft Windows	
megasas (megasas)	Stopped/Manual	C:\WINDOWS\system32\drivers\megasas.sys	Avago Technologies	Microsoft Windows	
megasr (megasr)	Stopped/Manual	C:\WINDOWS\system32\drivers\megasr.sys	LSI Corporation, Inc.	Microsoft Windows	
mlx4_bus (Mellanox ConnectX Bus Enumerator)	Stopped/Manual	C:\WINDOWS\system32\drivers\mlx4_bus.sys	Mellanox	Microsoft Windows	
MMCSS (Multimedia Class Scheduler)	Running/Auto	C:\WINDOWS\system32\drivers\mmcss.sys	Microsoft Corporation	Microsoft Windows	
Modem (Modem)	Stopped/Manual	C:\WINDOWS\system32\drivers\modem.sys	Microsoft Corporation	Microsoft Windows	
monitor (Microsoft Monitor Class Function Driver Service)	Running/Manual	C:\WINDOWS\system32\drivers\monitor.sys	Microsoft Corporation	Microsoft Windows	
mouclass (Mouse Class Driver)	Running/Manual	C:\WINDOWS\system32\drivers\mouclass.sys	Microsoft Corporation	Microsoft Windows	
mouhid (Mouse HID Driver)	Running/Manual	C:\WINDOWS\system32\drivers\mouhid.sys	Microsoft Corporation	Microsoft Windows	
mountmgr (Mount Point Manager)	Running/Boot	C:\WINDOWS\system32\drivers\mountmgr.sys	Microsoft Corporation	Microsoft Windows	
mpsdrv (Windows Firewall Authorization Driver)	Running/Manual	C:\WINDOWS\system32\drivers\mpsdrv.sys	Microsoft Corporation	Microsoft Windows	
MRxDAV (WebDav Client Redirector Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\mrxdav.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb (SMB MiniRedirector Wrapper and Engine)	Running/Manual	C:\WINDOWS\system32\drivers\mrxsmb.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb10 (SMB 1.x MiniRedirector)	Running/Auto	C:\WINDOWS\system32\drivers\mrxsmb10.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb20 (SMB 2.0 MiniRedirector)	Running/Manual	C:\WINDOWS\system32\drivers\mrxsmb20.sys	Microsoft Corporation	Microsoft Windows	
MsBridge (Microsoft MAC Bridge)	Stopped/Manual	C:\WINDOWS\system32\drivers\bridge.sys	Microsoft Corporation	Microsoft Windows	
msgpiowin32 (Common Driver for Buttons, DockMode and Laptop/Slate Indicator)	Stopped/Manual	C:\WINDOWS\system32\drivers\msgpiowin32.sys	Microsoft Corporation	Microsoft Windows	
mshidkmdf (Pass-	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
through HID to KMDF Filter Driver)		32\drivers\mshidkmdf.sys			
mshidumdf (Pass-through HID to UMDF Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\mshidumdf.sys	Microsoft Corporation	Microsoft Windows	
msisadrv (msisadrv)	Running/Boot	C:\WINDOWS\system32\drivers\msisadrv.sys	Microsoft Corporation	Microsoft Windows	
MSKSSRV (Microsoft Streaming Service Proxy)	Stopped/Manual	C:\WINDOWS\system32\drivers\mskssrv.sys	Microsoft Corporation	Microsoft Windows	
MsLldp (Microsoft Link-Layer Discovery Protocol)	Running/Auto	C:\WINDOWS\system32\drivers\mslldp.sys	Microsoft Corporation	Microsoft Windows	
MSPCLOCK (Microsoft Streaming Clock Proxy)	Stopped/Manual	C:\WINDOWS\system32\drivers\mspclock.sys	Microsoft Corporation	Microsoft Windows	
MSPQM (Microsoft Streaming Quality Manager Proxy)	Stopped/Manual	C:\WINDOWS\system32\drivers\mspqm.sys	Microsoft Corporation	Microsoft Windows	
mssmbios (Microsoft System Management BIOS Driver)	Running/System	C:\WINDOWS\system32\drivers\mssmbios.sys	Microsoft Corporation	Microsoft Windows	
MSTEE (Microsoft Streaming Tee/Sink-to-Sink Converter)	Stopped/Manual	C:\WINDOWS\system32\drivers\mstee.sys	Microsoft Corporation	Microsoft Windows	
MTConfig (Microsoft Input Configuration Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\MTConfig.sys	Microsoft Corporation	Microsoft Windows	
Mup (Mup)	Running/Boot	C:\WINDOWS\system32\drivers\mup.sys	Microsoft Corporation	Microsoft Windows	
mvumis (mvumis)	Stopped/Manual	C:\WINDOWS\system32\drivers\mvumis.sys	Marvell Semiconductor, Inc.	Microsoft Windows	
NativeWifiP (NativeWiFi Filter)	Stopped/Manual	C:\WINDOWS\system32\drivers\nwifi.sys	Microsoft Corporation	Microsoft Windows	
ndfltr (NetworkDirect Service)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndfltr.sys	Mellanox	Microsoft Windows	
NDIS (NDIS System Driver)	Running/Boot	C:\WINDOWS\system32\drivers\ndis.sys	Microsoft Corporation	Microsoft Windows	
NdisCap (Microsoft NDIS Capture)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndiscap.sys	Microsoft Corporation	Microsoft Windows	
NdisImPlatform (Microsoft Network Adapter Multiplexor Protocol)	Stopped/Manual	C:\WINDOWS\system32\drivers\NdisImPlatform.sys	Microsoft Corporation	Microsoft Windows	
NdisTapi (Remote Access NDIS TAPI Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndistapi.sys	Microsoft Corporation	Microsoft Windows	
Ndisuio (NDIS Usermode I/O Protocol)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndisuio.sys	Microsoft Corporation	Microsoft Windows	
NdisVirtualBus (Microsoft Virtual Network Adapter Enumerator)	Running/Manual	C:\WINDOWS\system32\drivers\NdisVirtualBus.sys	Microsoft Corporation	Microsoft Windows	
NdisWan (Remote Access NDIS WAN Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndiswan.sys	Microsoft Corporation	Microsoft Windows	
ndiswanlegacy (Remote Access LEGACY NDIS WAN Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\ndiswan.sys	Microsoft Corporation	Microsoft Windows	
ndproxy (@	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
%SystemRoot %\system32\drivers\todo.sys,-101;NDIS Proxy)		32\drivers\ndproxy.sys			
Ndu (Windows Network Data Usage Monitoring Driver)	Running/Auto	C:\WINDOWS\system32\drivers\Ndu.sys	Microsoft Corporation	Microsoft Windows	
NetBIOS (NetBIOS Interface)	Running/System	C:\WINDOWS\system32\drivers\netbios.sys	Microsoft Corporation	Microsoft Windows	
NetBT (NetBT)	Running/System	C:\WINDOWS\system32\drivers\netbt.sys	Microsoft Corporation	Microsoft Windows	
npsvctrig (Named pipe service trigger provider)	Running/System	C:\WINDOWS\system32\drivers\npsvctrig.sys	Microsoft Corporation	Microsoft Windows	
nsiproxy (NSI Proxy Service Driver)	Running/System	C:\WINDOWS\system32\drivers\nsiproxy.sys	Microsoft Corporation	Microsoft Windows	
nv_agp (NVIDIA nForce AGP Bus Filter)	Stopped/Manual	C:\WINDOWS\system32\drivers\NV_AGP.SYS	Microsoft Corporation	Microsoft Windows	
nvraid (nvraid)	Stopped/Manual	C:\WINDOWS\system32\drivers\nvraid.sys	NVIDIA Corporation	Microsoft Windows	
nvstor (nvstor)	Stopped/Manual	C:\WINDOWS\system32\drivers\nvstor.sys	NVIDIA Corporation	Microsoft Windows	
Parport (Parallel port driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\parport.sys	Microsoft Corporation	Microsoft Windows	
partmgr (Partition Manager)	Running/Boot	C:\WINDOWS\system32\drivers\partmgr.sys	Microsoft Corporation	Microsoft Windows	
pci (PCI Bus Driver)	Running/Boot	C:\WINDOWS\system32\drivers\pci.sys	Microsoft Corporation	Microsoft Windows	
pciide (pciide)	Stopped/Manual	C:\WINDOWS\system32\drivers\pciide.sys	Microsoft Corporation	Microsoft Windows	
pcmcia (pcmcia)	Stopped/Manual	C:\WINDOWS\system32\drivers\pcmcia.sys	Microsoft Corporation	Microsoft Windows	
pcw (Performance Counters for Windows Driver)	Running/Boot	C:\WINDOWS\system32\drivers\pcw.sys	Microsoft Corporation	Microsoft Windows	
pdc (pdc)	Running/Boot	C:\WINDOWS\system32\drivers\pdc.sys	Microsoft Corporation	Microsoft Windows	
PEAUTH (PEAUTH)	Running/Auto	C:\WINDOWS\system32\drivers\PEAuth.sys	Microsoft Corporation	Microsoft Windows	
percsas2i (percsas2i)	Stopped/Manual	C:\WINDOWS\system32\drivers\percsas2i.sys	LSI Corporation	Microsoft Windows	
percsas3i (percsas3i)	Stopped/Manual	C:\WINDOWS\system32\drivers\percsas3i.sys	Avago Technologies	Microsoft Windows	
PNPMEM (Microsoft Memory Module Driver)	Running/Manual	C:\WINDOWS\system32\drivers\pnpmem.sys	Microsoft Corporation	Microsoft Windows	
PptpMiniport (WAN Miniport (PPTP))	Stopped/Manual	C:\WINDOWS\system32\drivers\raspptp.sys	Microsoft Corporation	Microsoft Windows	
Processor (Processor Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\processr.sys	Microsoft Corporation	Microsoft Windows	
Psched (QoS Packet Scheduler)	Running/System	C:\WINDOWS\system32\drivers\pacer.sys	Microsoft Corporation	Microsoft Windows	
QWAVEdrv (QWAVE driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\qwavedrv.sys	Microsoft Corporation	Microsoft Windows	
RasAcd (Remote Access Auto Connection Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\rasacd.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
RasAgileVpn (WAN Miniport (IKEv2))	Stopped/Manual	C:\WINDOWS\system32\drivers\agilevpn.sys	Microsoft Corporation	Microsoft Windows	
Rasl2tp (WAN Miniport (L2TP))	Stopped/Manual	C:\WINDOWS\system32\drivers\rasl2tp.sys	Microsoft Corporation	Microsoft Windows	
RasPppoe (Remote Access PPPOE Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\raspppoe.sys	Microsoft Corporation	Microsoft Windows	
RasSstp (WAN Miniport (SSTP))	Stopped/Manual	C:\WINDOWS\system32\drivers\rassstp.sys	Microsoft Corporation	Microsoft Windows	
rdbss (Redirected Buffering Sub System)	Running/System	C:\WINDOWS\system32\drivers\rdbss.sys	Microsoft Corporation	Microsoft Windows	
rdpbus (Remote Desktop Device Redirector Bus Driver)	Running/Manual	C:\WINDOWS\system32\drivers\rdpbus.sys	Microsoft Corporation	Microsoft Windows	
RDPDR (Remote Desktop Device Redirector Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\rdpdr.sys	Microsoft Corporation	Microsoft Windows	
RdpVideoMiniport (Remote Desktop Video Miniport Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\rdpvideominiport.sys	Microsoft Corporation	Microsoft Windows	
rdyboost (ReadyBoost)	Running/Boot	C:\WINDOWS\system32\drivers\rdyboost.sys	Microsoft Corporation	Microsoft Windows	
rspndr (Link-Layer Topology Discovery Responder)	Running/Auto	C:\WINDOWS\system32\drivers\rspndr.sys	Microsoft Corporation	Microsoft Windows	
s3cap (s3cap)	Stopped/Manual	C:\WINDOWS\system32\drivers\vms3cap.sys	Microsoft Corporation	Microsoft Windows	
sbp2port (SBP-2 Transport/Protocol Bus Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\sbp2port.sys	Microsoft Corporation	Microsoft Windows	
scfilter (Smart card PnP Class Filter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\scfilter.sys	Microsoft Corporation	Microsoft Windows	
sdbus (sdbus)	Stopped/Manual	C:\WINDOWS\system32\drivers\sdbus.sys	Microsoft Corporation	Microsoft Windows	
sdstor (SD Storage Port Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\sdstor.sys	Microsoft Corporation	Microsoft Windows	
SensorsHIDClassDriver (UMDF Reflector service for Sensors HID Class Driver)	Running/Manual	C:\WINDOWS\system32\drivers\WUDFRd.sys	Microsoft Corporation	Microsoft Windows	
SerCx (Serial UART Support Library)	Stopped/Manual	C:\WINDOWS\system32\drivers\SerCx.sys	Microsoft Corporation	Microsoft Windows	
SerCx2 (Serial UART Support Library)	Stopped/Manual	C:\WINDOWS\system32\drivers\SerCx2.sys	Microsoft Corporation	Microsoft Windows	
Serenum (Serenum Filter Driver)	Running/Manual	C:\WINDOWS\system32\drivers\serenum.sys	Microsoft Corporation	Microsoft Windows	
Serial (Serial port driver)	Running/Manual	C:\WINDOWS\system32\drivers\serial.sys	Microsoft Corporation	Microsoft Windows	
sermouse (Serial Mouse Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\sermouse.sys	Microsoft Corporation	Microsoft Windows	
sfloppy (High-Capacity Floppy Disk Drive)	Stopped/Manual	C:\WINDOWS\system32\drivers\sfloppy.sys	Microsoft Corporation	Microsoft Windows	
SiSRaid2 (SiSRaid2)	Stopped/Manual	C:\WINDOWS\system32\drivers\sisraid2.sys	Silicon Integrated Systems Corp.	Microsoft Windows	
SiSRaid4 (SiSRaid4)	Stopped/Manual	C:\WINDOWS\system32\drivers\sisraid4.sy	Silicon Integrated Systems	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
		s			
spaceport (Storage Spaces Driver)	Running/Boot	C:\WINDOWS\system32\drivers\spaceport.sys	Microsoft Corporation	Microsoft Windows	
SpbCx (Simple Peripheral Bus Support Library)	Stopped/Manual	C:\WINDOWS\system32\drivers\SpbCx.sys	Microsoft Corporation	Microsoft Windows	
srv (Server SMB 1.xxx Driver)	Running/Auto	C:\WINDOWS\system32\drivers\srv.sys	Microsoft Corporation	Microsoft Windows	
srv2 (Server SMB 2.xxx Driver)	Running/Manual	C:\WINDOWS\system32\drivers\srv2.sys	Microsoft Corporation	Microsoft Windows	
srvnet (srvnet)	Running/Manual	C:\WINDOWS\system32\drivers\srvnet.sys	Microsoft Corporation	Microsoft Windows	
stexstor (stexstor)	Stopped/Manual	C:\WINDOWS\system32\drivers\stexstor.sys	Promise Technology, Inc.	Microsoft Windows	
storahci (Microsoft Standard SATA AHCI Driver)	Running/Boot	C:\WINDOWS\system32\drivers\storahci.sys	Microsoft Corporation	Microsoft Windows	
storflt (Microsoft Hyper-V Storage Accelerator)	Stopped/Manual	C:\WINDOWS\system32\drivers\vmstorfl.sys	Microsoft Corporation	Microsoft Windows	
stornvme (Microsoft Standard NVM Express Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\stornvme.sys	Microsoft Corporation	Microsoft Windows	
storqosflt (Storage QoS Filter Driver)	Running/Auto	C:\WINDOWS\system32\drivers\storqosflt.sys	Microsoft Corporation	Microsoft Windows	
storufs (Microsoft Universal Flash Storage (UFS) Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\storufs.sys	Microsoft Corporation	Microsoft Windows	
storvsc (storvsc)	Stopped/Manual	C:\WINDOWS\system32\drivers\storvsc.sys	Microsoft Corporation	Microsoft Windows	
swenum (Software Bus Driver)	Running/Manual	C:\WINDOWS\system32\drivers\swenum.sys	Microsoft Corporation	Microsoft Windows	
Synth3dVsc (Synth3dVsc)	Stopped/Manual	C:\WINDOWS\system32\drivers\Synth3dVsc.sys	Microsoft Corporation	Microsoft Windows	
Tcpip (TCP/IP Protocol Driver)	Running/Boot	C:\WINDOWS\system32\drivers\tcpip.sys	Microsoft Corporation	Microsoft Windows	
Tcpip6 (@todo.dll,-100;Microsoft IPv6 Protocol Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\tcpip.sys	Microsoft Corporation	Microsoft Windows	
tcpipreg (TCP/IP Registry Compatibility)	Running/Auto	C:\WINDOWS\system32\drivers\tcpipreg.sys	Microsoft Corporation	Microsoft Windows	
tdx (NetIO Legacy TDI Support Driver)	Running/System	C:\WINDOWS\system32\drivers\tdx.sys	Microsoft Corporation	Microsoft Windows	
terminpt (Microsoft Remote Desktop Input Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\terminpt.sys	Microsoft Corporation	Microsoft Windows	
TPM (TPM)	Stopped/Manual	C:\WINDOWS\system32\drivers\tpm.sys	Microsoft Corporation	Microsoft Windows	
tsusbflt (Remote Desktop USB Hub Class Filter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\TsUsbFlt.sys	Microsoft Corporation	Microsoft Windows	
TsUsbGD (Remote Desktop Generic USB Device)	Stopped/Manual	C:\WINDOWS\system32\drivers\TsUsbGD.sys	Microsoft Corporation	Microsoft Windows	
tunnel (Microsoft Tunnel Miniport Adapter Driver)	Running/Manual	C:\WINDOWS\system32\drivers\tunnel.sys	Microsoft Corporation	Microsoft Windows	
uagp35 (Microsoft	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
AGPv3.5 Filter)		32\drivers\UAGP35.SYS			
UASPStor (USB Attached SCSI (UAS) Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\uaspstor.sys	Microsoft Corporation	Microsoft Windows	
UcmCx0101 (USB Connector Manager KMDF Class Extension)	Stopped/Manual	C:\WINDOWS\system32\drivers\UcmCx.sys	Microsoft Corporation	Microsoft Windows	
UcmUcsi (USB Connector Manager UCSI Client)	Stopped/Manual	C:\WINDOWS\system32\drivers\UcmUcsi.sys	Microsoft Corporation	Microsoft Windows	
Ucx01000 (USB Host Support Library)	Running/Manual	C:\WINDOWS\system32\drivers\UCX01000.SYS	Microsoft Corporation	Microsoft Windows	
UdeCx (USB Device Emulation Support Library)	Stopped/Manual	C:\WINDOWS\system32\drivers\Udecx.sys	Microsoft Corporation	Microsoft Windows	
udfs (udfs)	Stopped/Disabled	C:\WINDOWS\system32\drivers\udfs.sys	Microsoft Corporation	Microsoft Windows	
UEFI (Microsoft UEFI Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\uefi.sys	Microsoft Corporation	Microsoft Windows	
Ufx01000 (USB Function Class Extension)	Stopped/Manual	C:\WINDOWS\system32\drivers\ufx01000.sys	Microsoft Corporation	Microsoft Windows	
UfxChipidea (USB Chipidea Controller)	Stopped/Manual	C:\WINDOWS\system32\drivers\UfxChipidea.sys	Microsoft Corporation	Microsoft Windows	
ufxsynopsys (USB Synopsys Controller)	Stopped/Manual	C:\WINDOWS\system32\drivers\ufxsynopsys.sys	Microsoft Corporation	Microsoft Windows	
uliagpkx (Uli AGP Bus Filter)	Stopped/Manual	C:\WINDOWS\system32\drivers\ULIAGPKX.SYS	Microsoft Corporation	Microsoft Windows	
umbus (UMBus Enumerator Driver)	Running/Manual	C:\WINDOWS\system32\drivers\umbus.sys	Microsoft Corporation	Microsoft Windows	
UmPass (Microsoft UMPass Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\umpass.sys	Microsoft Corporation	Microsoft Windows	
UrsChipidea (Chipidea USB Role-Switch Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\urschipidea.sys	Microsoft Corporation	Microsoft Windows	
UrsCx01000 (USB Role-Switch Support Library)	Stopped/Manual	C:\WINDOWS\system32\drivers\urscx01000.sys	Microsoft Corporation	Microsoft Windows	
UrsSynopsys (Synopsys USB Role-Switch Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\urssynopsys.sys	Microsoft Corporation	Microsoft Windows	
usbccgp (Microsoft USB Generic Parent Driver)	Running/Manual	C:\WINDOWS\system32\drivers\usbccgp.sys	Microsoft Corporation	Microsoft Windows	
usbcir (eHome Infrared Receiver (USBCIR))	Stopped/Manual	C:\WINDOWS\system32\drivers\usbcir.sys	Microsoft Corporation	Microsoft Windows	
usbehci (Microsoft USB 2.0 Enhanced Host Controller Miniport Driver)	Running/Manual	C:\WINDOWS\system32\drivers\usbehci.sys	Microsoft Corporation	Microsoft Windows	
usbhub (Microsoft USB Standard Hub Driver)	Running/Manual	C:\WINDOWS\system32\drivers\usbhub.sys	Microsoft Corporation	Microsoft Windows	
USBHUB3 (SuperSpeed Hub)	Running/Manual	C:\WINDOWS\system32\drivers\USBHUB3.SYS	Microsoft Corporation	Microsoft Windows	
usbohci (Microsoft	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
USB Open Host Controller Miniport Driver)		32\drivers\usbohci.sys			
usbprint (Microsoft USB PRINTER Class)	Stopped/Manual	C:\WINDOWS\system32\drivers\usbprint.sys	Microsoft Corporation	Microsoft Windows	
usbser (Microsoft USB Serial Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\usbser.sys	Microsoft Corporation	Microsoft Windows	
USBSTOR (USB Mass Storage Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\USBSTOR.SYS	Microsoft Corporation	Microsoft Windows	
usbuhci (Microsoft USB Universal Host Controller Miniport Driver)	Running/Manual	C:\WINDOWS\system32\drivers\usbuhci.sys	Microsoft Corporation	Microsoft Windows	
USBXHCI (USB xHCI Compliant Host Controller)	Running/Manual	C:\WINDOWS\system32\drivers\USBXHCI.SYS	Microsoft Corporation	Microsoft Windows	
vdrvroot (Microsoft Virtual Drive Enumerator)	Running/Boot	C:\WINDOWS\system32\drivers\vdrvroot.sys	Microsoft Corporation	Microsoft Windows	
VerifierExt (VerifierExt)	Stopped/Manual	C:\WINDOWS\system32\drivers\VerifierExt.sys	Microsoft Corporation	Microsoft Windows	
vhdmp (vhdmp)	Stopped/Manual	C:\WINDOWS\system32\drivers\vhdmp.sys	Microsoft Corporation	Microsoft Windows	
vhf (Virtual HID Framework (VHF) Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\vhf.sys	Microsoft Corporation	Microsoft Windows	
vm3dmp (vm3dmp)	Running/Manual	C:\WINDOWS\system32\drivers\vm3dmp.sys	VMware, Inc.	VMware, Inc.	
vmbus (Virtual Machine Bus)	Stopped/Manual	C:\WINDOWS\system32\drivers\vmbus.sys	Microsoft Corporation	Microsoft Windows	
VMBusHID (VMBusHID)	Stopped/Manual	C:\WINDOWS\system32\drivers\VMBusHID.sys	Microsoft Corporation	Microsoft Windows	
vmci (VMware VMCI Bus Driver)	Running/Boot	C:\WINDOWS\system32\drivers\vmci.sys	VMware, Inc.	VMware, Inc.	
vmhgfs (VMware Host Guest Client Redirector)	Running/System	C:\WINDOWS\system32\drivers\vmhgfs.sys	VMware, Inc.	VMware, Inc.	
VMMEMCTL (Memory Control Driver)	Running/Auto	C:\Program Files\Common Files\VMware\Drivers\memctl\vmmemctl.sys	VMware, Inc.	VMware, Inc.	☹ quote ImagePath
vmmouse (VMware Pointing Device)	Running/Manual	C:\WINDOWS\system32\drivers\vmmouse.sys	VMware, Inc.	VMware, Inc.	
vmrawdsk (VMware Vista Physical Disk Helper)	Running/System	C:\Program Files\VMware\VMware Tools\vmrawdsk.sys	VMware, Inc.	VMware, Inc.	☹ quote ImagePath
VMUsbMouse (VMware USB Pointing Device)	Running/Manual	C:\WINDOWS\system32\drivers\vmusbmouse.sys	VMware, Inc.	VMware, Inc.	
volmgr (Volume Manager Driver)	Running/Boot	C:\WINDOWS\system32\drivers\volmgr.sys	Microsoft Corporation	Microsoft Windows	
volmgrx (Dynamic Volume Manager)	Running/Boot	C:\WINDOWS\system32\drivers\volmgrx.sys	Microsoft Corporation	Microsoft Windows	
volsnap (Storage volumes)	Running/Boot	C:\WINDOWS\system32\drivers\volsnap.sys	Microsoft Corporation	Microsoft Windows	
vpci (Microsoft Hyper-V Virtual PCI Bus)	Stopped/Manual	C:\WINDOWS\system32\drivers\vpci.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
vsmraid (vsmraid)	Stopped/Manual	C:\WINDOWS\system32\drivers\vsmraid.sys	VIA Technologies Inc.,Ltd	Microsoft Windows	
vsock (vSockets Driver)	Running/Boot	C:\WINDOWS\system32\drivers\vsock.sys	VMware, Inc.	VMware, Inc.	
VSTXRAID (VIA StorX Storage RAID Controller Windows Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\VSTXRAID.SYS	VIA Corporation	Microsoft Windows	
vwifibus (Virtual Wi-Fi Bus Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\vwifibus.sys	Microsoft Corporation	Microsoft Windows	
vwififlt (Virtual WiFi Filter Driver)	Running/System	C:\WINDOWS\system32\drivers\vwififlt.sys	Microsoft Corporation	Microsoft Windows	
WacomPen (Wacom Serial Pen HID Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\wacompen.sys	Microsoft Corporation	Microsoft Windows	
wanarp (Remote Access IP ARP Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\wanarp.sys	Microsoft Corporation	Microsoft Windows	
wanarpv6 (Remote Access IPv6 ARP Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\wanarp.sys	Microsoft Corporation	Microsoft Windows	
WdBoot (Windows Defender Boot Driver)	Stopped/Boot	C:\WINDOWS\system32\drivers\WdBoot.sys	Microsoft Corporation	Microsoft Windows	
Wdf01000 (Kernel Mode Driver Frameworks service)	Running/Boot	C:\WINDOWS\system32\drivers\Wdf01000.sys	Microsoft Corporation	Microsoft Windows	
WdFilter (Windows Defender Mini-Filter Driver)	Running/Boot	C:\WINDOWS\system32\drivers\WdFilter.sys	Microsoft Corporation	Microsoft Windows	
wdiwifi (WDI Driver Framework)	Stopped/Manual	C:\WINDOWS\system32\drivers\WdiWiFi.sys	Microsoft Corporation	Microsoft Windows	
WdNisDrv (Windows Defender Network Inspection System Driver)	Running/Manual	C:\WINDOWS\system32\drivers\WdNisDrv.sys	Microsoft Corporation	Microsoft Windows	
WFPLWFS (Microsoft Windows Filtering Platform)	Running/Boot	C:\WINDOWS\system32\drivers\wfplwfs.sys	Microsoft Corporation	Microsoft Windows	
WIMMount (WIMMount)	Stopped/Manual	C:\WINDOWS\system32\drivers\wimmount.sys	Microsoft Corporation	Microsoft Windows	
WindowsTrustedRT (Windows Trusted Execution Environment Class Extension)	Running/Boot	C:\WINDOWS\system32\drivers\WindowsTrustedRT.sys	Microsoft Corporation	Microsoft Windows	
WindowsTrustedRTProxy (Microsoft Windows Trusted Runtime Secure Service)	Running/Boot	C:\WINDOWS\system32\drivers\WindowsTrustedRTProxy.sys	Microsoft Corporation	Microsoft Windows	
WinMad (WinMad Service)	Stopped/Manual	C:\WINDOWS\system32\drivers\winmad.sys	Mellanox	Microsoft Windows	
WINUSB (WinUsb Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\winusb.sys	Microsoft Corporation	Microsoft Windows	
WinVerbs (WinVerbs Service)	Stopped/Manual	C:\WINDOWS\system32\drivers\winverbs.sys	Mellanox	Microsoft Windows	
WmiAcpi (Microsoft Windows Management Interface for ACPI)	Stopped/Manual	C:\WINDOWS\system32\drivers\wmiacpi.sys	Microsoft Corporation	Microsoft Windows	
wpcfltr (Family Safety	Stopped/Manual	C:\WINDOWS\system	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Filter Driver)		32\drivers\wpcfltr.sys			
WpdUpFltr (WPD Upper Class Filter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\WpdUpFltr.sys	Microsoft Corporation	Microsoft Windows	
ws2ifsl (Winsock IFS Driver)	Stopped/Disabled	C:\WINDOWS\system32\drivers\ws2ifsl.sys	Microsoft Corporation	Microsoft Windows	
WudfPf (User Mode Driver Frameworks Platform Driver)	Running/Manual	C:\WINDOWS\system32\drivers\WUDFPf.sys	Microsoft Corporation	Microsoft Windows	
WUDFRd (WUDFRd)	Running/Manual	C:\WINDOWS\system32\drivers\WUDFRd.sys	Microsoft Corporation	Microsoft Windows	
xboxgip (Xbox Game Input Protocol Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\xboxgip.sys	Microsoft Corporation	Microsoft Windows	
xinputhid (XINPUT HID Filter Driver)	Stopped/Manual	C:\WINDOWS\system32\drivers\xinputhid.sys	Microsoft Corporation	Microsoft Windows	

[Computer W10W] [Top][Summary][Explanatory notes]

1.3.3 [SVCS-03] Services and drivers access permissions

The check verifies access permissions (ACLs) of system services and drivers. The check fails if there is a service with non-std. owner, or there is a service whose configuration can be modified by non-privileged users, or there is a service which can be started/stopped by an anonymous user. Exceptions can be defined by check parameters if necessary. Services which fail to satisfy the above rules are shown in the results table together with detailed specifications of the problem.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

1.3.4 [SVCS-04] Service accounts

The check verifies privilege level of accounts, which are used to run system services. If the account of any service falls into one of the privilege levels defined by the check parameters, the overall result of the check is **FAIL**. Exceptions can be defined by other parameters if necessary. Results table lists the problematic services, the account under which they are executed and its privilege level.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

1.3.5 [SVCS-05] Other programs that run automatically

The check verifies access permissions for programs that are just running, that are runnable via PATH environment variable, or that are executed automatically, without direct user action. The permissions must not allow program to be modified by unprivileged users for a successful test result. Exceptions can be specified by check parameters if necessary.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

1.4 [SECP-xx] Security policy

1.4.1 [SECP-01] Passwords and account locking policy

Check verifies the given passwords and accounts locking parameters. Parameters not listed in the profile are not checked.

Check result: FAIL.

We recommend to use the Group Policy to modify these settings. Domain-wide policy object (typically the Default Domain Policy) has to be modified to change the domain accounts policy; for the member servers and workstations local accounts, the policy objects linked to subordinate OU levels can be used as well. GPO settings path is

Computer Configuration(/Policies)/Windows Settings/Security Settings/Account Policies (and further either *Password Policy* or *Account Lockout Policy* depending on the particular setting).

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter name	Value	Recommendation
Min password length	0	min. 8
Max password age (d)	42	
Min password age (d)	0	min. 1
Password history length	0	min. 5
Store passwords using reversible encryption	0	
Password must meet complexity requirements	0	1
Account lockout duration (min)	30	
Reset account lockout counter after (min)	30	
Account lockout threshold	no locking	max. 10

[Computer W10W] [Top][Summary][Explanatory notes]

1.4.2 [SECP-02] Security settings

Check verifies the current settings of the specified system security options.

Check result: FAIL.

Using the Group Policy is recommended to modify these settings. The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Local Policies/Security Options*.

Note: We strongly recommend thorough testing of the new settings before changing the values in production environment, especially in the case of the parameters affecting network traffic. Potentially the most problematic settings are indicated in table by "[!]".

Security options being verified are listed in the table below. Problematic values are marked in red:

Category	Parameter name	Value	Recommendation
Accounts	Block Microsoft accounts		users can't add or log on with microsoft accounts
	Guest account status	Disabled	
	Limit local account use of blank passwords to console logon only	Enabled	
Devices	Prevent users from installing printer drivers	Disabled	enabled
Interactive logon	Do not require CTRL+ALT+DEL		disabled
	Machine inactivity limit		5-15 min
	Number of previous logons to cache (in case domain controller is not available)	10	0 or 1
Microsoft network client	Digitally sign communications (if server agrees)	Enabled	
	Send unencrypted password to third-party SMB servers	Disabled	
Microsoft network server	Digitally sign communications (always)	Disabled	enabled [!]
	Digitally sign communications (if client agrees)	Disabled	enabled
Network access	Allow anonymous SID/Name translation	Disabled	
	Do not allow anonymous enumeration of SAM accounts	Enabled	
	Do not allow anonymous enumeration of SAM accounts and shares	Disabled	enabled [!]
	Do not allow storage of passwords and credentials for network authentication	Disabled	enabled [!]
	Let Everyone permissions apply to anonymous users	Disabled	

Category	Parameter name	Value	Recommendation
	Restrict anonymous access to Named Pipes and Shares	Enabled	
	Sharing and security model for local accounts	Classic: Local users authenticate as themselves	
Network security	Do not store LAN Manager hash value on next password change	Enabled	
	LAN Manager authentication level		<any variant refusing LM auth> [!]
System objects	Require case insensitivity for non-Windows subsystems	Enabled	
	Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
User Account Control	Admin Approval Mode for the Built-in Administrator account		enabled
	Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	
	Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	prompt for consent/credentials on the secure desktop
	Only elevate executables that are signed and validated	Disabled	
	Only elevate UIAccess applications that are installed in secure locations	Enabled	
	Run all administrators in Admin Approval Mode	Enabled	
	Switch to the secure desktop when prompting for elevation	Enabled	
	Virtualize file and registry write failures to per-user locations	Enabled	

[Computer W10W] [Top][Summary][Explanatory notes]

1.4.3 [SECP-03] Audit settings

The check verifies if the configuration of the system security audit meets the minimum defined by parameters. The check is designed to test the audit settings by subcategories, which are supported on Windows 6.x (ie. Windows Vista and higher). Category-based settings used on older systems is not verified.

Check result: FAIL.

The use of Group policy is recommended to modify audit settings. The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Advanced Audit Policy Configuration*.

Note: Although the audit subcategories are supported on Windows 6.0 (ie. Windows Vista and Windows Server 2008), these systems do not support audit subcategory management through Group Policy. Subcategory-based audit settings on these systems can only be changed locally using command line utility *auditpol* or using third-party solutions. Group Policy support is implemented only in Windows 6.1 systems (Windows 7, Windows Server 2008/R2) and higher.

Current audit settings are listed in the table. Subcategories with the audit level lower than required are marked in red.

Category	Subcategory	Value	Recommendation
Account Logon	Credential Validation	No auditing	Success + Failure
	Kerberos Authentication Service	No auditing	
	Kerberos Service Ticket Operations	No auditing	
	Other Account Logon Events	No auditing	
Account Management	Application Group Management	No auditing	
	Computer Account Management	No auditing	Success + Failure
	Distribution Group Management	No auditing	

Category	Subcategory	Value	Recommendation
	Other Account Management Events	No auditing	Success + Failure
	Security Group Management	Success	Success + Failure
	User Account Management	Success	Success + Failure
Detailed Tracking	DPAPI Activity	No auditing	
	Plug and Play Events	No auditing	
	Process Creation	No auditing	min. Success
	Process Termination	No auditing	
	RPC Events	No auditing	
DS Access	Detailed Directory Service Replication	No auditing	
	Directory Service Access	No auditing	
	Directory Service Changes	No auditing	
	Directory Service Replication	No auditing	
Logon/Logoff	Account Lockout	Success	Success + Failure
	Group Membership	No auditing	
	IPsec Extended Mode	No auditing	
	IPsec Main Mode	No auditing	
	IPsec Quick Mode	No auditing	
	Logoff	Success	
	Logon	Success	Success + Failure
	Network Policy Server	Success, Failure	
	Other Logon/Logoff Events	No auditing	
	Special Logon	Success	
	User / Device Claims	No auditing	
Object Access	Application Generated	No auditing	
	Central Access Policy Staging	No auditing	
	Certification Services	No auditing	
	Detailed File Share	No auditing	
	File Share	No auditing	
	File System	No auditing	min. Failure
	Filtering Platform Connection	No auditing	
	Filtering Platform Packet Drop	No auditing	
	Handle Manipulation	No auditing	
	Kernel Object	No auditing	
	Other Object Access Events	No auditing	
	Registry	No auditing	min. Failure
	Removable Storage	No auditing	Success + Failure
	SAM	No auditing	
Policy Change	Audit Policy Change	Success	Success + Failure
	Authentication Policy Change	Success	Success + Failure
	Authorization Policy Change	No auditing	Success + Failure
	Filtering Platform Policy Change	No auditing	
	MPSSVC Rule-Level Policy Change	No auditing	
	Other Policy Change Events	No auditing	
Privilege Use	Non Sensitive Privilege Use	No auditing	
	Other Privilege Use Events	No auditing	
	Sensitive Privilege Use	No auditing	Success + Failure
System	IPsec Driver	No auditing	Success + Failure
	Other System Events	Success, Failure	
	Security State Change	Success	Success + Failure
	Security System Extension	No auditing	Success + Failure
	System Integrity	Success, Failure	

[Computer W10W] [Top][Summary][Explanatory notes]

1.4.4 [SECP-04] Parameters of log files

Check performs validation of log files parameters. The check is only successful when all three standard logs (application, system, security) are rewritten as needed, their files are stored in the system directory subtree, and the minimal size of each log and its recording time window complies with the check parameters. Furthermore, the guest access to event logs is required to be disabled for systems older than Windows 2003, and the total size of all the logs should not exceed 300 MB for systems older than Windows Vista.

Check result: OK WITH WARNING.

These settings can be modified locally, by changing the relevant parameters in the properties of the EventLog using application (mmc snap-in) *Event Viewer*. But in the case of domain computers we rather recommend using Group Policy object (the path to the relevant settings in the GPO is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Event Log*); however, this option is not available in the local GP object (eg. standalone machines).

Log files parameters are listed in the table below. Problematic values are marked in red:

Log	Parameter	Value	Recommendation
Application	Filename	%SystemRoot %\system32\winevt\Logs\Application.evtx	
	Retention	Overwrite as needed	
	Log size	20.0 MB	
Security	Filename	%SystemRoot %\System32\winevt\Logs\Security.evtx	
	Retention	Overwrite as needed	
	Log size	20.0 MB	☹ min. 60 MB
System	Filename	%SystemRoot %\system32\winevt\Logs\System.evtx	
	Retention	Overwrite as needed	
	Log size	20.0 MB	

[Computer W10W] [Top][Summary][Explanatory notes]

1.4.5 [SECP-05] Other security settings

Check verifies various security parameters of the system not included in other chapters. It is checked whether the Autorun is disabled and if the Windows Error Reporting is disabled; also, correct processing of the Group Policy is verified on domain members.

Check result: FAIL.

Errors in Group Policy objects application are usually due to inadequate configuration of the system components or due to problems at the infrastructure level (server is inaccessible due to the filtration on network elements, permissions do not allow access to network share, etc.). The solution is therefore usually more complicated; system event log may be helpful under some circumstances.

Autorun can be disabled either locally or through an Group Policy object (the GPO setting path is *Computer Configuration/Administrative Templates/System* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/AutoPlay Policies* [Vista+]) (related link: Autorun and autologon).

Windows Error Reporting can be disabled either locally or through an Group Policy object (the GPO setting path is *Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/Windows Error Reporting* [Vista+]) (related link: Error reporting).

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter	Value	Recommendation
Autorun	Enabled (for computer), disabled in all 2 user profiles	disable
Wake lock	Enabled in all power modes (locally)	
Screen lock	Disabled (for computer) (settings insufficient in all 2 user profiles)	enable (no more than 900 s)
Diagnostic and usage data	Full (locally)	disable

Parameter	Value	Recommendation
Windows Defender: Cloud-based protection	Enabled (locally)	☹ disable
Windows Defender: Sample submission	Enabled (locally)	disable

[Computer W10W] [Top][Summary][Explanatory notes]

1.4.6 [SECP-06] Privacy

Check verifies several settings affecting the user privacy, which are available on Windows 10.

Check result: OK WITH WARNING.

The values to be verified are listed in the table below. Problematic values are marked in red:

Category	Parameter name	Value	Recommendation
Advertising ID usage	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
SmartScreen filter	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
Send info about writing	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
Online search (Bing)	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
Speech, inking & typing	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
Location	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	none	
Camera	State	enabled in 1 profiles (out of 2): W10W\John Doe	☹ consider globally disabling in all profiles
	Authorized applications	8 applications total: Microsoft.Appconnector (W10W\John Doe), Microsoft.BioEnrollment (W10W\John Doe), Microsoft.Messaging (W10W\John Doe), Microsoft.MicrosoftEdge (W10W\John Doe), Microsoft.Office.OneNote (W10W\John Doe), Microsoft.Office.Sway (W10W\John Doe), Microsoft.WindowsCamera (W10W\John Doe), Microsoft.WindowsMaps (W10W\John Doe)	☹ consider the necessity of authorized applications
Microphone	State	enabled in 1 profiles (out of 2): W10W\John Doe	☹ consider globally disabling in all profiles
	Authorized applications	8 applications total: Microsoft.BioEnrollment (W10W\John Doe), Microsoft.Messaging (W10W\John Doe), Microsoft.MicrosoftEdge (W10W\John Doe), Microsoft.Office.Sway (W10W\John Doe), Microsoft.Windows.Cortana (W10W\John Doe), Microsoft.WindowsCamera (W10W\John Doe), Microsoft.WindowsSoundRecorder (W10W\John Doe), Microsoft.XboxApp (W10W\John Doe)	☹ consider the necessity of authorized applications
Account info	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	none	

Category	Parameter name	Value	Recommendation
Contacts	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	7 applications total: Microsoft.Appconnector (W10W\John Doe), Microsoft.CommsPhone (W10W\John Doe), Microsoft.Messaging (W10W\John Doe), Microsoft.People (W10W\John Doe), Microsoft.Windows.Cortana, Microsoft.Windows.ShellExperienceHost, microsoft.windowscommunicationsapps	☹ consider the necessity of authorized applications
Calendar	State	enabled in 1 profiles (out of 2): W10W\John Doe	☹ consider globally disabling in all profiles
	Authorized applications	4 applications total: Microsoft.Appconnector (W10W\John Doe), Microsoft.CommsPhone (W10W\John Doe), Microsoft.Windows.Cortana (W10W\John Doe), microsoft.windowscommunicationsapps (W10W\John Doe)	☹ consider the necessity of authorized applications
Messaging	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	3 applications total: Microsoft.CommsPhone (W10W\John Doe), Microsoft.Messaging (W10W\John Doe), Microsoft.Windows.Cortana	☹ consider the necessity of authorized applications
Radios	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	none	
Other devices	State	enabled in all 2 profiles	☹ consider globally disabling in all profiles
	Authorized applications	none	

[Computer W10W] [Top][Summary][Explanatory notes]

1.5 [USER-xx] User accounts

1.5.1 [USER-01] System-wide privileges

The check verifies that the specified system privileges are not held by anybody outside the defined range of allowable holders. If there is a privilege held by unauthorized user or group, the overall outcome of the check is **FAIL**. Privilege holders are listed in the results table.

Check result: FAIL.

The unauthorized privilege holders can basically only be removed by using Group Policy (if we do not consider third party tools or eg. utilities from the Resource Kit). GPO path to the appropriate settings is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Local Policies/User Rights Assignment*.

The table shows the privilege holders. Conflicting privilege assignments are marked in red:

Privilege	Holder(s)	Recommendation
Access Credential Manager as a trusted caller (SeTrustedCredManAccessPrivilege)		
Act as part of the operating system (SeTcbPrivilege)		
Allow log on locally (SeInteractiveLogonRight)	W10W\Administrators, W10W\Backup Operators, W10W\Users	

Privilege	Holder(s)	Recommendation
	W10W\Guest, W10W\System Managed Accounts Group	☹ remove privilege holder(s)
Allow log on through Remote Desktop Services (SeRemoteInteractiveLogonRight)	W10W\Administrators, W10W\Remote Desktop Users	
Back up files and directories (SeBackupPrivilege)	W10W\Administrators, W10W\Backup Operators	
Create a token object (SeCreateTokenPrivilege)		
Debug programs (SeDebugPrivilege)	W10W\Administrators	☹ remove privilege holder(s)
Deny access to this computer from the network (SeDenyNetworkLogonRight)	W10W\Guest	
	(not assigned: built-in administrator account)	☹ assign privilege holder(s)
Deny log on locally (SeDenyInteractiveLogonRight)	W10W\Guest	
Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)		
Force shutdown from a remote system (SeRemoteShutdownPrivilege)	W10W\Administrators	
Impersonate a client after authentication (SeImpersonatePrivilege)	W10W\Administrators, W10W\LOCAL SERVICE, W10W\NETWORK SERVICE, W10W\SERVICE	
Load and unload device drivers (SeLoadDriverPrivilege)	W10W\Administrators	
Manage auditing and security log (SeSecurityPrivilege)	W10W\Administrators	
Modify an object label (SeRelabelPrivilege)		
Restore files and directories (SeRestorePrivilege)	W10W\Administrators	
	W10W\Backup Operators	remove privilege holder(s)
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	W10W\Administrators	

[Computer W10W] [Top][Summary][Explanatory notes]

1.5.2 [USER-02] Problematic active accounts

The check inspects security-related attributes of user accounts. The active accounts, for which any of the following conditions are true, are considered risky: an account's password does not expire, an account has a password older than one year, an account has a password older than policy limit, an account's password is empty or weak or it cannot be changed, account is locked, account has expired, account is marked trusted for delegation, account may authenticate without Kerberos pre-authentication, account has password stored under reversible encryption, or an account has not logged in during the last year. Problematic accounts are listed in the results table. Exceptions can be defined by the check parameters if necessary.

Check result: FAIL.

The table lists the problematic accounts, which have been detected:

Problem	Account
No password expiration	W10W\Jane Doe
	W10W\John Doe
Password older than policy limit	W10W\Jane Doe
	W10W\John Doe

[Computer W10W] [Top][Summary][Explanatory notes]

1.5.3 [USER-03] Local groups membership

The check verifies whether groups specified by the parameters contain other than explicitly permitted members. The group membership is not evaluated transitively for the purpose of this inspection.

Check result: FAIL.

The listed group members should be removed from the respective groups. This can be done either by modifying the groups directly on the relevant computer or the Group Policy can be used to enforce group membership (Restricted

Groups). The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Restricted Groups*.

The table lists the groups with unauthorized members and the unauthorized members themselves:

Group	Member(s)	Recommendation
W10W\Administrators	W10W\Administrator	
	W10W\John Doe	remove member(s)
W10W\Backup Operators		
W10W\Network Configuration Operators		
W10W\Power Users		
W10W\Remote Desktop Users		

[Computer W10W] [Top][Summary][Explanatory notes]

1.5.4 [USER-04] Logon cache

The check reviews the content of the logon cache. The overall result of the check is **FAIL** if there is password verifier recorded in the cache which belongs to a domain account with permissions outside of the current server/workstation. The logon cache entries are listed in the result table.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

1.6 [ACLS-xx] Access control

1.6.1 [ACLS-01] File system of local drives

The check verifies whether all local disks use NTFS as its filesystem. In the case there exists a local drive that does not meet this condition the overall check result is **FAIL**. The offending drives and their details are given in the results table.

Check result: OK.

Of course, the filesystem type cannot be changed centraly. The drive has to be reformatted directly on the given server/station.

Mount point	Volume label/Size	Filesystem	Recommendation
C:\	-- / 29.5 GB	NTFS	

[Computer W10W] [Top][Summary][Explanatory notes]

1.6.2 [ACLS-02] File access permissions

The check verifies access permissions (ACLs) of important files and directories. For the successful outcome of the check there may be no file with non-std. owner, no file may have null DACL, and no file may be writable by unprivileged users. Exceptions can be defined by the check parameters if necessary. Files and folders not satisfying the above rules are listed in the results table together with the detailed problem specification.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

1.7 [NETW-xx] Network settings

1.7.1 [NETW-01] Global settings

The check verifies the setting of basic network parameters. For the check to be successful the following conditions must be true: NetBIOS has to be disabled on all network interfaces, IP routing has to be disabled, built-in firewall has to be enabled and system configuration files hosts a lmhosts.sam have to be empty (each of these tests can be disabled by the check parameters if necessary).

Check result: FAIL.

These settings (except for the built-in firewall configuration) cannot be managed centrally using Group Policy; values have to be set manually on each server/workstation. The GPO path for Windows built-in firewall settings is *Computer Configuration(/Policies)/Administrative Templates/Network/Network Connections/Windows Firewall*.

Related links:

- Disabling NetBIOS
- Hosts and lmhosts.sam files

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter	Value	Recommendation
NetBIOS	Enabled on 172.22.8.136	disable
Installed firewall software	(Windows built-in firewall)	
Current firewall status	Enabled	
IP Routing	Disabled	
System 'hosts' file	Empty	
System 'lmhosts.sam' file	Empty	
Wi-Fi Sense: Open hotspots	(no Wi-Fi interface)	
Wi-Fi Sense: Password sharing	(no Wi-Fi interface)	

[Computer W10W] [Top][Summary][Explanatory notes]

1.7.2 [NETW-02] Problematic open TCP/UDP ports

Check verifies the open external (not loopback) ports, both TCP and UDP, against the specified set of rules.

Check result: OK WITH WARNING.

Disabling/limiting the accessibility of open ports usually means to stop the service, or to change its configuration (loopback binding), or to filter IP traffic eg. by using the built-in firewall or IPSec filters. It is usually local action that is difficult to centralize (but there are the exceptions - eg. firewall configuration).

Important notice: Windows built-in firewall is enabled on the computer. Its state is not taken into account.

The table lists the blacklisted TCP/UDP ports that are open on external interfaces:

Protocol	Port	Local address	Process	Recommendation
TCP	135	*	884 (svchost.exe - RpcSs)	
TCP6	135	*	884 (svchost.exe - RpcSs)	
TCP	139	172.22.8.136	4 (System)	limit the access
TCP	445	*	4 (System)	
TCP6	445	*	4 (System)	
UDP	137	172.22.8.136	4 (System)	limit the access
UDP	138	172.22.8.136	4 (System)	limit the access
UDP	1900	172.22.8.136	988 (svchost.exe - SSDPSRV)	
UDP6	1900	FE80::8CEB:5768:714E:2005%5	988 (svchost.exe - SSDPSRV)	
UDP	3544	*	540 (svchost.exe - iphlpsvc)	
UDP	3702	*	1060 (svchost.exe - EventSystem)	
UDP6	3702	*	988 (svchost.exe - FDResPub)	

[Computer W10W] [Top][Summary][Explanatory notes]

1.7.3 [NETW-03] System server components configuration

The check validates some basic parameters of the computer's server components. The two components to be checked are Terminal Server (security level, encryption, in-session password entering) and SNMP service (app-level IP filtering, authentication trap settings and defined communities).

Check result: OK.

The configuration of both server components can be done through Group policy; the GPO path to the appropriate settings is *Computer Configuration(/Policies)/Administrative Templates/Network/SNMP* and *Computer Configuration/Administrative Templates/Windows Components/Terminal Services/Encryption and Security* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/Remote Desktop*

Services/Remote Desktop Session Host/Security [Vista+]. However, it should be noted that configuring the SNMP using Group policy can have the security implications, especially as for the definition of the SNMP communities.

Service	Parameter	Value	Recommendation
Terminal Server	Allow incomming connections	Disabled	

[Computer W10W] [Top][Summary][Explanatory notes]

1.7.4 [NETW-04] Shared resources

The check examines permissions for shared drives. For successful outcome of the check the following conditions have to be true: share has to have std. owner, it has to have non-null DACL, it may not allow access to anonymous users and it may not allow writting to a large non-privileged group (*Everyone*, *Authenticated Users*, *Users*, *Domain Users*) at both the share and the file system level (however, file system permissions check is performed only for the top-level directory of sharing). Exceptions can be specified by check parameters if necessary.

Check result: OK.

[Computer W10W] [Top][Summary][Explanatory notes]

2 EXPLANATORY NOTES

2.1 Classification of findings in results tables

Informational line, no finding.	(no recommendation)
Assessed parameter line, no finding (ok).	(no recommendation)
Assessed parameter line, lower severity finding (warning).	☹ text of recommendation
Assessed parameter line, important finding (error).	text of recommendation

2.2 Abbreviations used

Services access permissions

Null DACL	NULL DACL (no access restriction)
Owner	Owned by non-std. privileged group
ChgCfgACE	Non-std. privileged group can change service config
ExecACE	Anonymous can start/stop service

Security descriptor, the general structure

SD	Security descriptor
D:	Discretionary access list (DACL)
O:	Owner

Security descriptor, ACL flags

P	Protected
AR	Inheritance required
AI	Inherited

Security descriptor, ACE type

A	Allow
D	Deny
U	Audit
M	Mandatory label
OA	Object Allow
OD	Object Deny
OU	Object Audit

Security descriptor, ACE flags

CI	Container inherit
OI	Object inherit
IO	Inherit only
NP	Not propagate
ID	Inherited
SA	Success audit (SACL only)
FA	Failure audit (SACL only)

Security descriptor, ACE permissions

FC	Full control (cumulative)
WR	Write (cumulative)
RD	Read (cumulative)
EX	Execute (cumulative)
[Gfc]	Full control (generic)
[Gwr]	Write (generic)
[Grd]	Read (generic)
[Gex]	Execute (generic)

[Delete]	Delete (standard)
[Read_Ctrl]	Read control (standard)
[Write_DAC]	Write DACL (standard)
[Write_Owner]	Write owner (standard)
[Sync]	Synchronize (standard)
[SACL]	Access SACL (standard)

Security descriptor, permission holders (well-known security principals)

AN	Anonymous logon user
AO	Account operators
AU	Authenticated users
BA	Builtin (local) administrators
BG	Builtin (local) guests
BO	Backup operators
BU	Builtin (local) users
CG	Creator group
CO	Creator owner
ED	Enterprise domain controllers
HI	High mandatory level
IS	IUser
IU	Interactive logon user
LS	Local service
LU	Performance Log users
LW	Low mandatory level
ME	Medium mandatory level
MU	Performance Monitor users
mAA	Windows Authorization Access Group
mBL	Batch logon user
mCS	Creator group server
mDA	Digest Authentication
mDL	Dialup logon user
mNA	NTLM Authentication
mOO	Other Organization
mPX	Proxy
mRL	Remote logon
mSA	SChannel Authentication
mTB	Incoming Forest Trust Builders
mTL	Terminal Server License Servers
mTO	This organization
mTS	Terminal Server
NO	Network configuration operators (to manage configuration of networking features)
NS	Network service
NU	Nework logon user
PO	Printer operators
PS	Personal self
PU	Power users
RC	Restricted code
RD	Remote desktop users (for TS)
RE	Replicator
RU	Pre-windows 2000 compatible group
SI	System mandatory level
SO	Server operators
SU	Service logon user
SY	Local system
WD	Everyone (World)