Supported Images

Core STIG Hardening for Windows Guide

`harden-windows.ps1`

Windows Server 2019 | Windows Server 2022 | Windows Server 2025

Core security-hardening baseline for Supported Images Windows Server systems. Designed for unattended operation with backups, detailed logging, role-aware behavior, and configurable high-impact controls.

Document	Supported Images Core STIG Hardening for Windows Guide
Script	harden-windows.ps1
Copyright	Copyright 2026 Supported Images LLC. All rights reserved.

Version 1.0 | August 2026

1. Purpose and Scope

The Supported Images Core STIG Hardening for Windows script applies an unattended, reusable security-hardening baseline to supported Windows Server systems. The script is designed to strengthen common operating-system security controls while preserving practical server administration capabilities such as RDP, WinRM, Windows Update, domain membership, and role-specific operation.

The script supports Windows Server 2019, Windows Server 2022, and Windows Server 2025. It detects the operating system and whether the machine is standalone, domain joined, or a domain controller before applying role-sensitive settings.

Scope statement: This is a Supported Images "Core STIG Hardening" baseline. It is not presented as a complete DISA STIG remediation or compliance-certification tool. Full compliance can depend on server role, site policy, domain Group Policy, installed applications, certificates, firmware, network architecture, and environment-specific/manual controls.

1.1 Supported platforms

- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

1.2 Execution requirements

- Run from an elevated (Administrator) PowerShell session.
- Use 64-bit Windows PowerShell when the operating system is 64-bit so native policy registry locations are changed.
- PowerShell 5.1 or later is required by the script.
- The script runs unattended and does not display interactive confirmation prompts.

1.3 Normal execution

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -File .\harden-windows.ps1
```

When no parameters are supplied, the script uses its built-in defaults. Most hardening categories are enabled by default; the two deliberately high-impact controls—RDP drive-redirection blocking and Windows FIPS algorithm mode—are disabled by default.

2. Default Hardening Summary

Area	Default behavior
Operating-system detection	Confirms Windows Server 2019, 2022, or 2025; exits on unsupported versions.
Pre-change backups	Exports local security policy, Windows Firewall policy, and selected security registry keys.
Account policy	14-character minimum password, complexity, 24-password history, 60-day maximum age, 1-day minimum age; lockout threshold 3, duration/reset 15 minutes. Skipped on domain controllers.
Authentication / LSA	NTLMv2-only compatibility level, LM hash prevention, anonymous-access restrictions, blank-password restriction, WDigest credential caching disabled, LSA protected process enabled by default.
UAC	Enables UAC and secure-desktop elevation controls; hardens elevation behavior.
Network stack	Disables source routing and ICMP redirects, prevents NetBIOS name-release attacks, disables LLMNR.
SMB	Disables SMBv1, requires SMB signing, restricts null sessions, and blocks insecure guest authentication.
PowerShell	Disables PowerShell v2 when present; enables Script Block Logging, Module Logging, and command-line data in process-creation auditing.
Advanced auditing	Enables a broad set of System, Logon/Logoff, Object Access, Privilege Use, Detailed Tracking, Policy Change, Account Management, and Account Logon subcategories.
Event logs	Application 32 MB, Security 192 MB, System 32 MB; PowerShell Operational log enabled at 64 MB.
Microsoft Defender	Enables multiple Defender protections where available, including real-time, behavior, script, archive, IOAV, PUA, network protection, signature checks, MAPS, and safe sample submission.
Firewall	Enables Domain/Private/Public profiles; default inbound Block, outbound Allow; preserves existing allow rules and attempts to preserve active RDP/WinRM access.
RDP	Requires NLA, high encryption, TLS security layer, password prompt, encrypted RPC traffic, and disables Remote Assistance. Drive redirection remains allowed by default.
WinRM	Disables Basic authentication and unencrypted traffic for client and service policies.
TLS / SCHANNEL	Disables SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1; enables TLS 1.2 and .NET strong cryptography. Windows Server 2025 TLS 1.3 stays at OS default.
Windows Update	Enables automatic download/scheduled installation, daily scheduling at 3:00 AM, recommended updates, and no forced reboot while users are logged on. Existing WSUS policy is retained.
Services	Disables Remote Registry by default; disables Print Spooler on domain controllers.
Platform checks	Checks and logs Secure Boot and TPM state without attempting firmware or TPM provisioning changes.
Post-run inventory	Writes effective firewall, account, audit, SMB, Defender, RDP, and listening-port status to a timestamped hardening-status.txt file.

3. Logging, Backups, and Recovery Information

3.1 Primary hardening log

The default detailed action log is: C:\ProgramData\SupportedImages\Hardening\system-hardening.log

Every informational message, warning, failed setting attempt, and recorded configuration change is appended to this log with a UTC timestamp and severity level. At completion, the script records the number of changes/actions, warning count, backup directory, and reboot guidance.

3.2 Backup directory

```
C:\ProgramData\SupportedImages\Hardening\Backups\<UTC timestamp>\
```

A new timestamped directory is created for each run. The timestamp uses UTC in the format yyyyMMddTHHmmssZ.

Backup/status item	Purpose
security-policy-before.inf	Export of the pre-hardening local security policy using secedit.
firewall-before.wfw	Export of the pre-hardening Windows Defender Firewall policy using netsh advfirewall.
lsa-before.reg	Backup of HKLM\SYSTEM\CurrentControlSet\Control\Lsa.
smb-server-before.reg	Backup of LanmanServer parameters.
smb-client-before.reg	Backup of LanmanWorkstation parameters.
system-policies-before.reg	Backup of Windows CurrentVersion Policies\System.
windows-policies-before.reg	Backup of HKLM\SOFTWARE\Policies\Microsoft\Windows.
hardening-status.txt	Post-hardening status inventory generated after configuration completes.
work	Temporary security-template/database work area for account-policy application.

3.3 Firewall packet log

When firewall hardening is enabled, blocked-packet logging is enabled at:

```
%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
```

The firewall log maximum size is configured to 16,384 KB. Allowed-packet logging is not enabled by the script.

4. Detailed Hardening Actions

4.1 Operating-system and server-role detection

The script queries Win32_OperatingSystem and Win32_ComputerSystem. It identifies the Windows Server release from the operating-system caption and exits with an error if the system is not Windows Server 2019, 2022, or 2025.

The server role is also recorded. A domain role of 4 or higher is treated as a domain controller. If the server is domain joined, the script logs a warning that domain Group Policy can override local settings after the script runs.

4.2 Account and password policy

On standalone servers and member servers, the local security policy is configured as follows:

Setting	Value
Minimum password age	1 day
Maximum password age	60 days
Minimum password length	14 characters
Password complexity	Enabled
Password history	24 passwords
Account lockout threshold	3 failed attempts
Lockout duration	15 minutes
Reset lockout counter	15 minutes
Clear-text password storage	Disabled

Domain controller behavior: the local password and account-lockout template is intentionally skipped on domain controllers. Domain account policy should be controlled through domain Group Policy.

The built-in Guest account is disabled by default on non-domain-controller systems by locating the local account whose SID ends in -501.

4.3 Authentication, credential, and interactive-logon protection

- Sets LmCompatibilityLevel to 5, requiring NTLMv2 responses and refusing LM/NTLM responses.
- Prevents storage of LM password hashes (NoLMHash = 1).
- Restricts anonymous SAM enumeration and anonymous access.
- Removes Everyone-group inclusion for anonymous users.
- Restricts use of blank local-account passwords.
- Requires NTLM client and server session security values used by the script (NTLMMinClientSec and NTLMMinServerSec = 537395200).
- Disables WDigest UseLogonCredential so reusable credentials are not deliberately cached by that provider.
- Enables LSA protected-process mode (RunAsPPL) by default; this contributes to a reboot requirement.
- Does not display the last signed-in user.
- Requires Ctrl+Alt+Del (DisableCAD = 0).
- Sets the machine inactivity timeout to 900 seconds (15 minutes).

- Sets CachedLogonsCount to 4.
- Detects AutoAdminLogon or a stored DefaultPassword and logs a warning, but does not automatically delete those values.

4.4 User Account Control (UAC)

- UAC enabled (EnableLUA = 1).
- Elevation prompts use the secure desktop.
- Administrators are prompted for consent for elevation.
- Standard users are denied elevation requests rather than being allowed to enter alternate administrator credentials.
- Installer detection is enabled.
- UIAccess applications are restricted to secure locations.
- UIAccess applications cannot prompt for elevation without using the secure desktop.
- File/registry virtualization remains enabled for compatible legacy applications.

4.5 Network stack and name-resolution hardening

- IPv4 source routing disabled.
- IPv6 source routing disabled.
- ICMP redirects disabled.
- NetBIOS name-release-on-demand protection enabled.
- LLMNR multicast name resolution disabled.

4.6 SMB hardening

- SMBv1 disabled through registry configuration and SMB server configuration.
- SMBv1 optional Windows features are disabled when present.
- SMB server signing is enabled and required.
- SMB client signing is enabled and required.
- Null-session access is restricted.
- Insecure SMB guest authentication is disabled.

4.7 PowerShell hardening and PowerShell event logging

- Windows PowerShell 2.0 compatibility features are disabled when present.
- Script Block Logging is enabled.
- Script Block Invocation Logging is enabled.
- Module Logging is enabled for all modules (*).
- Process-creation audit events are configured to include command-line data.
- Microsoft-Windows-PowerShell/Operational is enabled and configured with a 64 MB maximum size.

4.8 Advanced audit policy

Advanced Audit Policy subcategories are forced to take precedence over legacy category-level audit policy. The script configures the following subcategories:

Category	Subcategory	Auditing
System	Security State Change	Success
System	Security System Extension	Success
System	System Integrity	Success + Failure

Category	Subcategory	Auditing
System	IPsec Driver	Success + Failure
System	Other System Events	Success + Failure
Logon/Logoff	Logon	Success + Failure
Logon/Logoff	Logoff	Success
Logon/Logoff	Account Lockout	Failure
Logon/Logoff	Special Logon	Success
Logon/Logoff	Other Logon/Logoff Events	Success + Failure
Logon/Logoff	Group Membership	Success
Object Access	File Share	Success + Failure
Object Access	Detailed File Share	Success + Failure
Object Access	Removable Storage	Success + Failure
Privilege Use	Sensitive Privilege Use	Success + Failure
Detailed Tracking	Process Creation	Success
Detailed Tracking	Process Termination	Success
Detailed Tracking	Plug and Play Events	Success
Policy Change	Audit Policy Change	Success + Failure
Policy Change	Authentication Policy Change	Success
Policy Change	Authorization Policy Change	Success
Policy Change	MPSSVC Rule-Level Policy Change	Success + Failure
Account Management	User Account Management	Success + Failure
Account Management	Computer Account Management	Success + Failure
Account Management	Security Group Management	Success + Failure
Account Management	Other Account Management Events	Success + Failure
Account Logon	Credential Validation	Success + Failure
Account Logon	Kerberos Service Ticket Operations	Success + Failure
Account Logon	Other Account Logon Events	Success + Failure
Account Logon	Kerberos Authentication Service	Success + Failure

Domain controllers additionally enable Directory Service Access and Directory Service Changes for both success and failure events.

4.9 Event log sizing

Log	Maximum size
Application	32 MB
Security	192 MB

Log	Maximum size
System	32 MB
PowerShell Operational	64 MB

4.10 Microsoft Defender and SmartScreen

When Microsoft Defender cmdlets are available, the script enables or configures the following:

- Real-time monitoring
- Behavior monitoring
- IOAV protection
- Script scanning
- Archive scanning
- Potentially unwanted application (PUA) protection
- Network protection
- Signature check before scans
- Microsoft MAPS advanced membership
- Safe sample submission
- WinDefend automatic startup and attempted service start
- SmartScreen enabled with Warn level

If Defender cmdlets are not present, Defender-specific changes are skipped and a warning is recorded; SmartScreen registry policy is still applied.

4.11 Windows Defender Firewall

Profile/behavior	Configuration
Domain profile	Enabled
Private profile	Enabled
Public profile	Enabled
Default inbound action	Block
Default outbound action	Allow
Notify on listen	Disabled
Blocked-packet logging	Enabled
Allowed-packet logging	Disabled
Firewall log size	16,384 KB

The script does not clear existing firewall rules. If RDP is currently enabled, it attempts to enable firewall rules associated with the TermService service. If WinRM is currently running, it attempts to enable firewall rules associated with WinRM. This is intended to reduce the risk of losing remote administrative access when the default inbound action is changed to Block.

Operational caution: firewall hardening changes the default inbound posture to Block. Existing application-specific allow rules are preserved, but operators should still validate required management and application connectivity before closing the current administrative session.

4.12 Remote Desktop hardening

- Network Level Authentication required (UserAuthentication = 1).
- Minimum encryption level set to High (MinEncryptionLevel = 3).
- RDP security layer set to TLS (SecurityLayer = 2).
- Password prompt required for connections.
- RPC traffic encryption required.
- Remote Assistance disabled.
- RDP drive redirection remains allowed by default; it can be disabled with -DisableRdpDriveRedirection $true.

4.13 WinRM hardening

- WinRM service policy: unencrypted traffic disabled.
- WinRM service policy: Basic authentication disabled.
- WinRM client policy: unencrypted traffic disabled.
- WinRM client policy: Basic authentication disabled.

4.14 TLS, SCHANNEL, and .NET cryptography

- SSL 2.0 disabled for SCHANNEL Client and Server.
- SSL 3.0 disabled for SCHANNEL Client and Server.
- TLS 1.0 disabled for SCHANNEL Client and Server.
- TLS 1.1 disabled for SCHANNEL Client and Server.
- TLS 1.2 explicitly enabled for SCHANNEL Client and Server.
- .NET Framework v4.0.30319 (64-bit and WOW6432Node) uses strong cryptography and system-default TLS versions.
- On Windows Server 2025, TLS 1.3 is left at the operating-system default rather than being explicitly changed.

Compatibility note: disabling TLS 1.0 and TLS 1.1 can affect legacy software and integrations. Use -EnableStrictTls $false when a known dependency still requires older protocols, then remediate that dependency separately.

4.15 Windows Update

- Automatic Updates enabled.
- Automatic download and scheduled installation (AUOptions = 4).
- ScheduledInstallDay = 0 (every day).
- ScheduledInstallTime = 3 (3:00 AM).
- No automatic reboot while users are logged on.
- Recommended updates included.
- Existing WSUS policy is not removed.

4.16 AutoRun and service hardening

AutoRun/AutoPlay is disabled for drive types by setting NoAutorun = 1 and NoDriveTypeAutoRun = 255.

Remote Registry is stopped and disabled by default when present. On domain controllers, the Print Spooler service is also stopped and disabled.

4.17 Secure Boot and TPM checks

The script checks Secure Boot status and TPM presence/readiness and records the result. It does not modify firmware configuration, enable Secure Boot, provision a TPM, or make other firmware-level changes.

5. Configuration Options

All Boolean options use PowerShell Boolean parameters. Supply $true or $false explicitly when changing a default. String options let you relocate the log and backup roots.

Parameter	Default	Effect
-EnableFirewall	$true	Enable firewall hardening on all profiles; inbound Block/outbound Allow; preserve existing rules.
-EnableAutomaticUpdates	$true	Configure Windows Update automatic download/scheduled installation policy.
-EnableDefenderHardening	$true	Apply Microsoft Defender and SmartScreen hardening when Defender cmdlets are available.
-EnableAccountPolicy	$true	Apply local password and lockout policy on non-DC systems.
-EnableAdvancedAudit	$true	Configure Advanced Audit Policy subcategories.
-EnablePowerShellLogging	$true	Enable Script Block/Invocation/Module logging and command-line process auditing.
-EnableSmbHardening	$true	Disable SMBv1, require SMB signing, restrict null/guest access.
-EnableUacHardening	$true	Apply UAC elevation and secure-desktop hardening.
-EnableRdpHardening	$true	Apply NLA, TLS/high encryption, password prompt, encrypted RPC, and Remote Assistance policy.
-EnableWinRmHardening	$true	Disable Basic authentication and unencrypted WinRM traffic for client/service.
-EnableStrictTls	$true	Disable SSL2/SSL3/TLS1.0/TLS1.1; enable TLS1.2 and .NET strong crypto.
-EnableLsaProtection	$true	Enable RunAsPPL protected-process mode for LSA.
-DisablePowerShellV2	$true	Disable PowerShell v2 optional compatibility components when present.
-DisableRemoteRegistry	$true	Stop and disable RemoteRegistry service when present.
-DisableGuestAccount	$true	Disable the built-in local Guest account on non-DC systems.
-DisableRdpDriveRedirection	$false	When true, prevent RDP client drive mapping/redirection.
-EnableFipsMode	$false	When true, enable Windows FIPS algorithm policy. High operational impact.
-LogFile	C:\ProgramData\SupportedImages\Hardening\system-hardening.log	Change the detailed action-log file location.
-BackupRoot	C:\ProgramData\SupportedImages\Hardening\Backups	Change the root directory used for timestamped backups/status output.

5.1 High-impact options

Disable RDP drive redirection

```
.\harden-windows.ps1 -DisableRdpDriveRedirection $true
```

Sets fDisableCdm = 1 under Terminal Services policy. This prevents client drive mapping through RDP and may affect administration, file transfer, or application workflows that rely on redirected drives.

Enable Windows FIPS mode

```
.\harden-windows.ps1 -EnableFipsMode $true
```

Enables the Windows FIPS algorithm policy and marks the run as requiring a reboot. The script logs an explicit warning because FIPS mode can cause compatibility problems with applications or cryptographic libraries that are not FIPS-aware.

5.2 Common customization examples

Run the complete default baseline

```
.\harden-windows.ps1
```

Leave legacy TLS configuration unchanged

```
.\harden-windows.ps1 -EnableStrictTls $false
```

Do not disable Remote Registry

```
.\harden-windows.ps1 -DisableRemoteRegistry $false
```

Do not change local password/lockout policy

```
.\harden-windows.ps1 -EnableAccountPolicy $false
```

Do not change firewall profiles/default actions

```
.\harden-windows.ps1 -EnableFirewall $false
```

Disable RDP drive redirection

```
.\harden-windows.ps1 -DisableRdpDriveRedirection $true
```

Enable FIPS mode

```
.\harden-windows.ps1 -EnableFipsMode $true
```

Use a custom action log

```
.\harden-windows.ps1 -LogFile "D:\Logs\system-hardening.log"
```

Use a custom backup root

```
.\harden-windows.ps1 -BackupRoot "D:\HardeningBackups"
```

6. Domain-Joined Servers and Domain Controllers

6.1 Domain-joined member servers

The script applies local hardening settings to domain-joined member servers, but records a warning that Group Policy can subsequently override them. The effective configuration should therefore be reviewed after domain policy refresh.

6.2 Domain controllers

When a domain controller is detected, the script changes behavior in several areas:

- Local password and account-lockout policy is not applied; domain account policy should be managed through domain GPO.
- Built-in local Guest account disabling logic is not executed.

- Directory Service Access auditing is enabled for success and failure.
- Directory Service Changes auditing is enabled for success and failure.
- Print Spooler is stopped and disabled.

7. Reboot Behavior and Post-Run Verification

The script does not automatically reboot the server. It tracks whether a reboot is required or strongly recommended and writes the result to the hardening log at completion.

A reboot flag is set by the script when changes such as LSA protection, TLS/SCHANNEL protocol changes, FIPS mode, or Windows optional-feature changes require it. The script also checks common Windows reboot-pending indicators and PendingFileRenameOperations.

7.1 Recommended verification sequence

1. Review C:\ProgramData\SupportedImages\Hardening\system-hardening.log for INFO, WARN, and ERROR entries.
2. Review the timestamped hardening-status.txt file for effective firewall, account, audit, SMB, Defender, RDP, and listening-port information.
3. Confirm required application ports and remote-management paths still function, especially after firewall and TLS changes.
4. On domain-joined machines, refresh/evaluate Group Policy and confirm that required local hardening settings were not overridden unexpectedly.
5. Schedule a reboot when the log reports that one is required or strongly recommended, then re-verify critical services and security settings.

7.2 Post-hardening status report

The status file includes:

- Operating system/version/build and domain role
- Firewall profiles and default actions
- Effective account policy from net accounts
- Complete Advanced Audit Policy output
- SMB server configuration
- Microsoft Defender status when available
- RDP security values
- Listening TCP ports

8. Operational Considerations and Exceptions

Area	Consideration
Group Policy	Domain GPO can override local settings. Validate effective policy after refresh.
Legacy TLS	Applications depending on TLS 1.0/1.1 can fail after default strict-TLS hardening.
Firewall	Inbound traffic is blocked by default unless an allow rule exists. Existing rules are preserved, but application connectivity must be validated.
RDP	The script attempts to preserve RDP firewall access if RDP is already enabled. Validate connectivity before ending the current session.
WinRM	Basic and unencrypted WinRM are disabled. Existing automation depending on either will need remediation.
SMB signing / SMBv1	Legacy systems or appliances that require unsigned SMB or SMBv1 may fail to connect.
FIPS mode	Off by default because enabling it can break non-FIPS-aware software.
RDP drive mapping	Allowed by default to preserve administrative workflows; can be disabled explicitly.
Defender	Defender-specific changes are skipped if Defender cmdlets are unavailable.
Secure Boot / TPM	The script only reports status; it does not alter firmware or provision a TPM.

9. Principal Configuration Locations

The script changes numerous registry policy locations and system settings. The following table identifies the principal areas modified. It is intended as an operational map rather than an exhaustive line-by-line registry reference.

Location / subsystem	Purpose
Local security policy	secedit security template for password/lockout policy on non-DC systems.
HKLM\SYSTEM\CurrentControlSet\Control\Lsa	Authentication compatibility, anonymous access restrictions, LSA protection, advanced audit override.
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0	NTLM client/server session-security minimums.
HKLM\...\SecurityProviders\WDigest	WDigest cached-logon credential behavior.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	Interactive-logon/UAC and process-creation command-line audit behavior.
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip*	IPv4/IPv6 source-routing and ICMP redirect settings.
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient	LLMNR configuration.
LanmanServer / LanmanWorkstation	SMB protocol/signing/null-session/guest behavior.
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell	PowerShell Script Block and Module Logging.
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog	Application, Security, and System log-size policy.
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	SmartScreen policy.
Windows Defender Firewall	Domain/Private/Public profile defaults and logging.
Terminal Server policy / RDP-Tcp	NLA, encryption, TLS security layer, password prompt, RPC encryption, Remote Assistance, optional drive redirection.
WinRM Client / Service policy	Basic authentication and unencrypted traffic.
SCHANNEL Protocols	SSL/TLS protocol enable/disable state for client and server.
.NET Framework v4.0.30319	Strong cryptography and system-default TLS version behavior.
WindowsUpdate\AU	Automatic update scheduling and reboot behavior.
Policies\Explorer	AutoRun/AutoPlay behavior.
Services	RemoteRegistry; Print Spooler on domain controllers.
FipsAlgorithmPolicy	Optional Windows FIPS mode.

10. Copyright, Confidentiality, and Use Restriction

The Supported Images Core STIG Hardening name describes the baseline implemented by the script. The script itself states that this baseline does not by itself constitute full DISA STIG compliance or certification.

END OF GUIDE