

10.71.108.114 ldr-trmprd114
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System -	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
■ User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.176 LDZ-WBSPRD02
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.179 LDZ-WBSPRD05
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.180 LDZ-WBSPRD06
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.131 lhipmdnprs01l1i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.132 lhipmdnprs02l1i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.133 LHIPMDNPRS03L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
■ User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.134 lhipmdnprs04l1i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.135 LHIPMDNPRS05L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.136 lhipmdnprs06l2i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.137 lhipmdnprs07l2i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.138 lhipmdnprs08l2i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.139 lhipmdnprs09l2i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.34.27 LHIPMdSgr03L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
■ User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.34.24 LHIPMdSgr04L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

200 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	190	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.	1	1	0
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.	1	1	0
	1	1	0
Simple TCP/IP Services must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.	0	0	1
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.	1	1	0
	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.	0	0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.63 LHIPMdWbs10L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.64 lhipmdnwbs11l1i
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.65 LHIPMdWbs12L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
Simple TCP/IP Services must not be installed.			
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.66 LHIPMdWbs13L1I
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

200 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	190	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.	1	1	0
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.	1	1	0
	1	1	0
Simple TCP/IP Services must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.	0	0	1
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.	1	1	0
	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.	0	0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.83 LHIPMdWbs14L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
Simple TCP/IP Services must not be installed.			
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.84 LHIPMdWbs15L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

200 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	190	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.	1	1	0
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.	1	1	0
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.	1	1	0
	1	1	0
Simple TCP/IP Services must not be installed.	1	1	0
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.	0	0	1
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.	1	1	0
	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.	0	0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1	● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●	
		● 1	● 0
	Indexing of encrypted files must be turned off.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Users must be prevented from changing installation options.	●	
		● 1	● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be notified if a web-based program attempts to install software.	●	
	SRG-OS-000480-GPOS-00229	● 1	● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	PowerShell script block logging must be enabled.	●	
	SRG-OS-000125-GPOS-00065	● 1	● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
	SRG-OS-000393-GPOS-00173	● 1	● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
	SRG-OS-000125-GPOS-00065	● 1	● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.85 LHIPMdWbs16L2I
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.70 LHIPMdWbs17L2I
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
Simple TCP/IP Services must not be installed.			
SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.49 LHIPMdWeb19L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.34 LHIPMdNWeb20L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.43 LHIPMdWeb21L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
■ User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
■ User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
■ User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.52 LHIPMdNWeb22L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000373-GPOS-00157	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.61 LHIPMdWeb23L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.70 LHIPMdNWeb24L1Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.55 LHIPMdNWeb25L2Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Other System Events failures.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security State Change successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - Security System Extension successes.	● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity successes.	● 1	● 0

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.133.64 LHIPMdNWeb26L2Z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.3.81 lhipopsftp01l1z
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1 ● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The display of slide shows on the lock screen must be disabled.	●
		● 1 ● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●
		● 1 ● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●
		● 1 ● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●
	SRG-OS-000420-GPOS-00186	● 1 ● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Insecure logons to an SMB server must be disabled.	●
		● 1 ● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	Command line data must be included in process creation events.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.104 lhi-trmprd104
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.	1	1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.	1	1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.	1	1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.	1	1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.	1	1	0
▼	1	1	0
Simple TCP/IP Services must not be installed.	1	1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.	0	0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.	1	1	0
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.	0	0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.84 LHIPMDNWBS15L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
■ Systems must be maintained at a supported servicing level.		1	0
▼ SRG-OS-000080-GPOS-00048	1	1	0
■ Local volumes must use a format that supports NTFS attributes.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Fax Server role must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	1	1	0
■ The Microsoft FTP service must not be installed unless required.		1	0
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The Peer Name Resolution Protocol must not be installed.		1	0
▼	1	1	0
■ Simple TCP/IP Services must not be installed.		1	0
▼ SRG-OS-000096-GPOS-00050	0	0	1
■ The Telnet Client must not be installed.		0	1
▼ SRG-OS-000095-GPOS-00049	1	1	0
■ The TFTP Client must not be installed.		1	0
▼	0	0	1
■ The Server Message Block (SMB) v1 protocol must be uninstalled.		0	1

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

172.19.2.133 SSVPMdnIvr01L11
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	● 0
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	● 0
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	● 0
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0
		● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

172.19.2.134 SSVPMdnIvr02L2I
Microsoft Windows Server 2016 Standard Edition 1607

97.03 % Compliant

1 Scanned Policies with 202 Rules

196 of 202 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2016 Mission Support Sensitive (Version 2, Revision 1)	196	196	6
▼ SRG-OS-000480-GPOS-00227	1	1	0
Systems must be maintained at a supported servicing level.			
▼ SRG-OS-000080-GPOS-00048	1	1	0
Local volumes must use a format that supports NTFS attributes.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Fax Server role must not be installed.			
▼ SRG-OS-000096-GPOS-00050	1	1	0
The Microsoft FTP service must not be installed unless required.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The Peer Name Resolution Protocol must not be installed.			
▼	1	1	0
Simple TCP/IP Services must not be installed.			
▼ SRG-OS-000096-GPOS-00050	0	0	1
The Telnet Client must not be installed.			
▼ SRG-OS-000095-GPOS-00049	1	1	0
The TFTP Client must not be installed.			
▼	0	0	1
The Server Message Block (SMB) v1 protocol must be uninstalled.			

		● 0 ● 1
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	●
	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	●
		● 1 ● 0
	Windows PowerShell 2.0 must not be installed.	●
	SRG-OS-000329-GPOS-00128	● 1 ● 0
	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	●
	SRG-OS-000021-GPOS-00005	● 1 ● 0
	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	●
		● 1 ● 0
	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	●
	SRG-OS-000077-GPOS-00045	● 1 ● 0
	Windows Server 2016 password history must be configured to 24 passwords remembered.	●
	SRG-OS-000076-GPOS-00044	● 1 ● 0
	Windows Server 2016 maximum password age must be configured to 60 days or less.	●
	SRG-OS-000075-GPOS-00043	● 1 ● 0
	Windows Server 2016 minimum password age must be configured to at least one day.	●
	SRG-OS-000078-GPOS-00046	● 1 ● 0
	Windows Server 2016 minimum password length must be configured to 14 characters.	●
	SRG-OS-000069-GPOS-00037	● 1 ● 0
	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	●

▼ SRG-OS-000073-GPOS-00041	● 1	● 0
Windows Server 2016 reversible password encryption must be disabled.	●	
▼ SRG-OS-000057-GPOS-00027	● 1	● 0
Permissions for the Application event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the Security event log must prevent access by non-privileged accounts.	●	
▼	● 1	● 0
Permissions for the System event log must prevent access by non-privileged accounts.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	●	

▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000240-GPOS-00090	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	●	
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	●	
▼	● 1	● 0
Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	●	
▼ SRG-OS-000327-GPOS-00127	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	●	
▼	● 1	● 0
Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	●	

	1 0
Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	1 0
Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver successes.	
	1 0
Windows Server 2016 must be configured to audit System - IPsec Driver failures.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events successes.	
	1 0
Windows Server 2016 must be configured to audit System - Other System Events failures.	
	1 0
Windows Server 2016 must be configured to audit System - Security State Change successes.	
	1 0
Windows Server 2016 must be configured to audit System - Security System Extension successes.	
	1 0
Windows Server 2016 must be configured to audit System - System Integrity successes.	

		● 1	● 0
	Windows Server 2016 must be configured to audit System - System Integrity failures.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The display of slide shows on the lock screen must be disabled.	●	
		● 1	● 0
	WDigest Authentication must be disabled on Windows Server 2016.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	●	
		● 1	● 0
	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	●	
		● 1	● 0
	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	●	
	SRG-OS-000420-GPOS-00186	● 1	● 0
	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Insecure logons to an SMB server must be disabled.	●	
		● 1	● 0
	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	●	
	SRG-OS-000042-GPOS-00020	● 1	● 0
	Command line data must be included in process creation events.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	●	

		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Downloading print driver packages over HTTP must be prevented.	●	
		● 1	● 0
	Printing over HTTP must be prevented.	●	
		● 1	● 0
	The network selection user interface (UI) must not be displayed on the logon screen.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (on battery).	●	
		● 1	● 0
	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
	SRG-OS-000368-GPOS-00154	● 1	● 0
	AutoPlay must be turned off for non-volume devices.	●	
		● 1	● 0
	The default AutoRun behavior must be configured to prevent AutoRun commands.	●	
		● 1	● 0
	AutoPlay must be disabled for all drives.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Administrator accounts must not be enumerated during elevation.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0

Windows Telemetry must be configured to Security or Basic.	1	0
SRG-OS-000341-GPOS-00132	1	0
The Application event log size must be configured to 32768 KB or greater.	1	0
▼	1	0
The Security event log size must be configured to 196608 KB or greater.	1	0
▼	1	0
The System event log size must be configured to 32768 KB or greater.	1	0
SRG-OS-000095-GPOS-00049	1	0
Windows Server 2016 Windows SmartScreen must be enabled.	1	0
SRG-OS-000433-GPOS-00192	1	0
Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
▼	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000373-GPOS-00157	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts.	1	0
SRG-OS-000373-GPOS-00157	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000250-GPOS-00093	1	0
The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	1	0

		● 1 ● 0
	Remote Desktop Services must be configured with the client connection encryption set to High Level.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Attachments must be prevented from being downloaded from RSS feeds.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	Basic authentication for RSS feeds over HTTP must not be used.	●
		● 1 ● 0
	Indexing of encrypted files must be turned off.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Users must be prevented from changing installation options.	●
		● 1 ● 0
	The Windows Installer Always install with elevated privileges option must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	Users must be notified if a web-based program attempts to install software.	●
	SRG-OS-000480-GPOS-00229	● 1 ● 0
	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	●
	SRG-OS-000042-GPOS-00020	● 1 ● 0
	PowerShell script block logging must be enabled.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0
	The Windows Remote Management (WinRM) client must not use Basic authentication.	●
	SRG-OS-000393-GPOS-00173	● 1 ● 0
	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●
	SRG-OS-000125-GPOS-00065	● 1 ● 0

<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) client must not use Digest authentication.	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not use Basic authentication.	1	0
<input checked="" type="checkbox"/> SRG-OS-000393-GPOS-00173	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	1	0
<input checked="" type="checkbox"/> SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	1	0
<input checked="" type="checkbox"/> SRG-OS-000112-GPOS-00057	1	0
<input checked="" type="checkbox"/> Kerberos user logon restrictions must be enforced.	1	0
<input checked="" type="checkbox"/> The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	1	0
<input checked="" type="checkbox"/> The Kerberos user ticket lifetime must be limited to 10 hours or less.	1	0
<input checked="" type="checkbox"/> The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	1	0
<input checked="" type="checkbox"/> The computer clock synchronization tolerance must be limited to 5 minutes or less.	1	0
<input checked="" type="checkbox"/> SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> Permissions on the Active Directory data files must only allow System and Administrators access.	1	0
<input checked="" type="checkbox"/> SRG-OS-000327-GPOS-00127	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	1	0

<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	1	0
<input checked="" type="checkbox"/> Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	1	0
SRG-OS-000423-GPOS-00187	1	0
<input checked="" type="checkbox"/> Domain controllers must require LDAP access signing.	1	0
SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Domain controllers must be configured to allow reset of machine account passwords.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	1	0
SRG-OS-000324-GPOS-00125	1	0
<input checked="" type="checkbox"/> The Add workstations to domain user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	1	0
SRG-OS-000080-GPOS-00048	1	0
<input checked="" type="checkbox"/> The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	1	0
SRG-OS-000080-GPOS-00048	1	0

<p>The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000297-GPOS-00115</p>	● 1	● 0
<p>The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.</p>	●	
<p>SRG-OS-000134-GPOS-00068</p>	● 1	● 0
<p>Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.</p>	●	
<p>SRG-OS-000095-GPOS-00049</p>	● 1	● 0
<p>Local users on domain-joined computers must not be enumerated.</p>	●	
<p>SRG-OS-000379-GPOS-00164</p>	● 1	● 0
<p>Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.</p>	●	
<p>SRG-OS-000480-GPOS-00227</p>	● 1	● 0
<p>Caching of logon credentials must be limited.</p>	●	
<p>SRG-OS-000324-GPOS-00125</p>	● 1	● 0
<p>Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.</p>	●	
<p>SRG-OS-000080-GPOS-00048</p>	● 1	● 0
<p>The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.</p>	●	
<p>The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.</p>	● 1	● 0
<p>The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.</p>	●	

	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	● 1	● 0
	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000297-GPOS-00115	● 1	● 0
	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	● 1	
	SRG-OS-000066-GPOS-00034	● 1	● 0
	The DoD Root CA certificates must be installed in the Trusted Root Store.	● 1	
	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	● 1	● 0
	SRG-OS-000121-GPOS-00062	● 1	● 0
	Windows Server 2016 built-in guest account must be disabled.	● 1	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	
	Windows Server 2016 built-in administrator account must be renamed.	● 1	● 0

Windows Server 2016 built-in guest account must be renamed.	1	0
SRG-OS-000062-GPOS-00031	1	0
Audit policy using subcategories must be enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	1	0
SRG-OS-000379-GPOS-00164	1	0
The computer account password must not be prevented from being reset.	1	0
SRG-OS-000480-GPOS-00227	1	0
The maximum age for machine account passwords must be configured to 30 days or less.	1	0
SRG-OS-000423-GPOS-00187	1	0
Windows Server 2016 must be configured to require a strong session key.	1	0
SRG-OS-000029-GPOS-00010	1	0
The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	1	0
SRG-OS-000423-GPOS-00187	1	0
The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	1	0

▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	●	
▼	● 1	● 0
■ The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous enumeration of shares must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ Anonymous access to Named Pipes and Shares must be restricted.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	●	
▼	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	●	

SRG-OS-000073-GPOS-00041	1	0
Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	1	0
SRG-OS-000480-GPOS-00227	1	0
The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	1	0
Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	1	0
Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000033-GPOS-00014	0	1
Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	0	1
SRG-OS-000480-GPOS-00227	1	0
The default permissions of global system objects must be strengthened.	1	0
SRG-OS-000373-GPOS-00157	1	0
User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	1	0

▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must automatically deny standard user requests for elevation.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must be configured to detect application installations and prompt for elevation.	●	
▼	● 1	● 0
User Account Control must only elevate UIAccess applications that are installed in secure locations.	●	
▼ SRG-OS-000373-GPOS-00157	● 1	● 0
User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
User Account Control must virtualize file and registry write failures to per-user locations.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	

	The Create permanent shared objects user right must not be assigned to any groups or accounts.	● 1	● 0
	The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
	The Debug programs user right must only be assigned to the Administrators group.	● 1	● 0
	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	● 1	● 0
	The Generate security audits user right must only be assigned to Local Service and Network Service.	● 1	● 0
	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
	The Increase scheduling priority user right must only be assigned to the Administrators group.	● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	● 1	● 0
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	● 1	● 0
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	● 1	● 0

	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Create a token object user right must not be assigned to any groups or accounts.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.12 ldr-ivrprd02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.14 ldr-ivrprd04
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.108 ldr-prsprd13
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.102.122 ldr-prsscp01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
 SRG-OS-000057-GPOS-00027	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
 SRG-OS-000324-GPOS-00125	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.104.34 ldr-sqlprd34
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.115 ldr-trmprd115
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.116 ldr-trmprd116
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.117 ldr-trmprd117
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.118 ldr-trmprd118
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.71.103.54

LDR-WBSPRD04

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.55

LDR-WBSPRD05

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.		0	1
	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.		0	1
	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.		0	1
	1	1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.59

LDR-WBSPRD09

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.46 LDR-WEBPRD04
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.17.33.199 LDZ-AUTHPRD01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.200 LDZ-AUTHPRD02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.197 LDZ-SIGRPRD01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.		0	1
	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.		0	1
	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.		0	1
	1	1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.196

LDZ-SIGRPRD02

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.177

LDZ-WBSPRD03

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.178 LDZ-WBSPRD04
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.189 LDZ-WEBPRD01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.190 LDZ-WEBPRD02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.130 LDZ-WEBPRD10
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.151 LDZ-WEBPRD11
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.142 ldz-webprd12
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.133 LDZ-WEBPRD13
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.154 LDZ-WEBPRD14
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.17.33.145 ldz-webprd15
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.136 LDZ-WEBPRD16
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.157 LDZ-WEBPRD17
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.17.33.138 LDZ-WEBPRD18
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.62.3.201 LHI-CLSQLPRD02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.71.106.11 lhi-ivrprd01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.13 lhi-ivrprd03
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.16 LHI-IVRPRD05
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.109 lhi-prsprd10
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.110 lhi-prsprd11
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.111 lhi-prsprd12
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.114 lhi-prsprd14
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.115 lhi-prsprd15
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.71.106.116 lhi-prsprd16
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.117 lhi-prsprd17
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.106.118 lhi-prsprd18
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.71.106.119 lhi-prsprd19
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.102.121 lhi-prsscp01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



		● 1	● 0
	The Load and unload device drivers user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Lock pages in memory user right must not be assigned to any groups or accounts.	●	
	SRG-OS-000057-GPOS-00027	● 1	● 0
	The Manage auditing and security log user right must only be assigned to the Administrators group.	●	
	SRG-OS-000324-GPOS-00125	● 1	● 0
	The Modify firmware environment values user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Profile single process user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Restore files and directories user right must only be assigned to the Administrators group.	●	
		● 1	● 0
	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	●	

10.71.104.30 lhi-sqlprd30
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

1

0

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.104.31 lhi-sqlprd31
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.104.33 lhi-sqlprd33
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.101 lhi-trmprd101
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.106 lhi-trmprd106
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.107 lhi-trmprd107
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.108 lhi-trmprd108
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.109 lhi-trmprd109
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.110 lhi-trmprd110
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.111 lhi-trmprd111
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.108.112 lhi-trmprd112
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.51 LHI-WBSPRD01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
The Allow log on locally user right must only be assigned to the Administrators group.	●	
The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
The Back up files and directories user right must only be assigned to the Administrators group.	●	
The Create a pagefile user right must only be assigned to the Administrators group.	● 1	● 0
The Create a token object user right must not be assigned to any groups or accounts.	●	
The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	● 1	● 0
The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
The Create symbolic links user right must only be assigned to the Administrators group.	● 1	● 0
The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.32 LHI-WBSPRD02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.24 LHI-WBSPRD03
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	0	1
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.50 LHI-WBSPRD06
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.60

LHI-WBSPRD07

Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	1	0
▼ SRG-OS-000064-GPOS-00033	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	1	0
▼	1	0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	1	0
▼ SRG-OS-000471-GPOS-00215	1	0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	1	0
▼	1	0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	1	0
▼ SRG-OS-000257-GPOS-00098	1	0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	1	0
▼ SRG-OS-000095-GPOS-00049	1	0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	1	0
▼	1	0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	1	0

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.61 LHI-WBSPRD08
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.40 LHI-WEBPRD01
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.43 LHI-WEBPRD02
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	0	0	1
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.	1	1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.	1	1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.	1	1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.	1	1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.	1	1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.	1	1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1	● 0
	Windows Peer-to-Peer networking services must be turned off.	●	
	Network Bridges must be prohibited in Windows.	●	
	SRG-OS-000134-GPOS-00068	● 1	● 0
	Domain users must be required to elevate when setting a networks location.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	All Direct Access traffic must be routed through the internal network.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The 6to4 IPv6 transition technology must be disabled.	●	
	The IP-HTTPS IPv6 transition technology must be disabled.	●	
	The ISATAP IPv6 transition technology must be disabled.	●	
	SRG-OS-000096-GPOS-00050	● 1	● 0
	The Teredo IPv6 transition technology must be disabled.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	IP stateless autoconfiguration limits state must be enabled.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●	
	The Windows Connect Now wizards must be disabled.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Windows Update must be prevented from searching for point and print drivers.	●	

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	

10.71.103.45 LHI-WEBPRD03
Microsoft Windows Server 2012 R2 Standard Edition

97.24 % Compliant

1 Scanned Policies with 254 Rules

247 of 254 Rules Passed

Policy Breakdown	Rules	Passed	Failed
DISA STIG Microsoft Windows Server 2012/2012 R2 Member Server Mission Support Sensitive (Version 3, Revision 1)	247	240	7
SRG-OS-000095-GPOS-00049	0	0	1
The Server Message Block (SMB) v1 protocol must be disabled on Windows 2012 R2.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			1
		0	1
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			1
		1	0
Windows PowerShell 2.0 must not be installed on Windows 2012/2012 R2.		1	0
SRG-OS-000329-GPOS-00128	1	1	0
Windows 2012 account lockout duration must be configured to 15 minutes or greater.		1	0
SRG-OS-000021-GPOS-00005	1	1	0
The number of allowed bad logon attempts must meet minimum requirements.		1	0
		1	0
The reset period for the account lockout counter must be configured to 15 minutes or greater on Windows 2012.		1	0
SRG-OS-000077-GPOS-00045	1	1	0
The password history must be configured to 24 passwords remembered.		1	0
SRG-OS-000076-GPOS-00044	1	1	0
The maximum password age must meet requirements.		1	0

▼ SRG-OS-000075-GPOS-00043	● 1	● 0
■ The minimum password age must meet requirements.	●	
▼ SRG-OS-000078-GPOS-00046	● 1	● 0
■ Passwords must, at a minimum, be 14 characters.	●	
▼ SRG-OS-000069-GPOS-00037	● 1	● 0
■ The built-in Windows password complexity policy must be enabled.	●	
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ Reversible password encryption must be disabled.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Logon - Credential Validation failures.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - Other Account Management Events successes.	●	
▼ SRG-OS-000004-GPOS-00004	● 1	● 0
■ The system must be configured to audit Account Management - Security Group Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management successes.	●	
▼	● 1	● 0
■ The system must be configured to audit Account Management - User Account Management failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
■ The system must be configured to audit Detailed Tracking - Process Creation successes.	●	
▼ SRG-OS-000470-GPOS-00214	● 1	● 0

<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout successes.	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit Logon/Logoff - Account Lockout failures.	● 1	● 0
▼ SRG-OS-000032-GPOS-00013	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logoff successes.	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon successes.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Logon failures.	● 1	● 0
▼ SRG-OS-000470-GPOS-00214	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Logon/Logoff - Special Logon successes.	● 1	● 0
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Audit Policy Change failures.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authentication Policy Change successes.	● 1	● 0
▼ SRG-OS-000474-GPOS-00219	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Policy Change - Authorization Policy Change successes.	● 1	● 0
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	●	
▼ SRG-OS-000064-GPOS-00033	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - IPsec Driver failures.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events successes.	●	
▼	● 1	● 0
<input type="checkbox"/> Windows Server 2012/2012 R2 must be configured to audit System - Other System Events failures.	●	
▼ SRG-OS-000471-GPOS-00215	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security State Change successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - Security System Extension successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity successes.	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to audit System - System Integrity failures.	●	
▼ SRG-OS-000257-GPOS-00098	● 1	● 0
<input type="checkbox"/> Event Viewer must be protected from unauthorized modification and deletion.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The Mapper I/O network protocol (LLTDIO) driver must be disabled.	●	
▼	● 1	● 0
<input type="checkbox"/> The Responder network protocol driver must be disabled.	●	

		● 1 ● 0
	Windows Peer-to-Peer networking services must be turned off.	●
	Network Bridges must be prohibited in Windows.	●
	SRG-OS-000134-GPOS-00068	● 1 ● 0
	Domain users must be required to elevate when setting a networks location.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	All Direct Access traffic must be routed through the internal network.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The 6to4 IPv6 transition technology must be disabled.	●
	The IP-HTTPS IPv6 transition technology must be disabled.	●
	The ISATAP IPv6 transition technology must be disabled.	●
	SRG-OS-000096-GPOS-00050	● 1 ● 0
	The Teredo IPv6 transition technology must be disabled.	●
	SRG-OS-000480-GPOS-00227	● 1 ● 0
	IP stateless autoconfiguration limits state must be enabled.	●
	SRG-OS-000095-GPOS-00049	● 1 ● 0
	The configuration of wireless devices using Windows Connect Now must be disabled.	●
	The Windows Connect Now wizards must be disabled.	●
	SRG-OS-000362-GPOS-00149	● 1 ● 0
	Windows Update must be prevented from searching for point and print drivers.	●

		● 1	● 0
	Optional component installation and component repair must be prevented from using Windows Update.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Remote access to the Plug and Play interface must be disabled for device installation.	●	
		● 1	● 0
	An Error Report must not be sent when a generic device driver is installed.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	A system restore point must be created when a new device driver is installed.	●	
	SRG-OS-000095-GPOS-00049	● 1	● 0
	Device metadata retrieval from the Internet must be prevented.	●	
		● 1	● 0
	Windows must be prevented from sending an error report when a device driver requests additional software during installation.	●	
	SRG-OS-000362-GPOS-00149	● 1	● 0
	Device driver searches using Windows Update must be prevented.	●	
		● 1	● 0
	Device driver updates must only search managed servers, not Windows Update.	●	
		● 1	● 0
	Users must not be prompted to search Windows Update for device drivers.	●	
	SRG-OS-000480-GPOS-00227	● 1	● 0
	Early Launch Antimalware, Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	●	
		● 1	● 0
	Group Policy objects must be reprocessed even if they have not changed.	●	
		● 1	● 0

<input type="checkbox"/> Group Policies must be refreshed in the background if the user is logged on.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Access to the Windows Store must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Downloading print driver packages over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Event Viewer Events.asp links must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	●	
▼	● 1	● 0
<input type="checkbox"/> The Internet File Association service must be turned off.	●	
▼	● 1	● 0
<input type="checkbox"/> Printing over HTTP must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> The Windows Customer Experience Improvement Program must be disabled.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
<input type="checkbox"/> Windows must be prevented from using Windows Update to search for drivers.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Copying of user input methods to the system account for sign-in must be prevented.	●	
▼	● 1	● 0
<input type="checkbox"/> Local users on domain-joined computers must not be enumerated.	●	
▼	● 1	● 0
<input type="checkbox"/> App notifications on the lock screen must be turned off.	●	

▼ SRG-OS-000373-GPOS-00156	● 1	● 0
■ Users must be prompted to authenticate on resume from sleep (on battery).	●	
▼	● 1	● 0
■ The user must be prompted to authenticate on resume from sleep (plugged in).	●	
▼ SRG-OS-000138-GPOS-00069	● 1	● 0
■ The system must be configured to prevent unsolicited remote assistance offers.	●	
▼	● 1	● 0
■ Solicited Remote Assistance must not be allowed.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Remote Assistance log files must be generated.	●	
▼ SRG-OS-000379-GPOS-00164	● 1	● 0
■ Unauthenticated RPC clients must be restricted from connecting to the RPC server.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ The detection of compatibility issues for applications and drivers must be turned off.	●	
▼	● 1	● 0
■ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	●	
▼	● 1	● 0
■ Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	●	
▼	● 1	● 0
■ Responsiveness events must be prevented from being aggregated and sent to Microsoft.	●	
▼	● 1	● 0
■ Trusted app installation must be enabled to allow for signed enterprise line of business apps.	●	
▼	● 1	● 0

<input type="checkbox"/> The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	●	
▼ SRG-OS-000368-GPOS-00154	● 1	● 0
<input type="checkbox"/> Autoplay must be turned off for non-volume devices.	●	
▼	● 1	● 0
<input type="checkbox"/> The default Autorun behavior must be configured to prevent Autorun commands.	●	
▼	● 1	● 0
<input type="checkbox"/> Autoplay must be disabled for all drives.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> The use of biometrics must be disabled.	●	
▼ SRG-OS-000079-GPOS-00047	● 1	● 0
<input type="checkbox"/> The password reveal button must not be displayed.	●	
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Administrator accounts must not be enumerated during elevation.	●	
▼ SRG-OS-000341-GPOS-00132	● 1	● 0
<input type="checkbox"/> The Application event log size must be configured to 32768 KB or greater.	●	
▼	● 0	● 1
<input type="checkbox"/> The Security event log size must be configured to 196608 KB or greater.		●
▼	● 1	● 0
<input type="checkbox"/> The Setup event log size must be configured to 32768 KB or greater.	●	
▼	● 1	● 0
<input type="checkbox"/> The System event log size must be configured to 32768 KB or greater.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
<input type="checkbox"/> Windows SmartScreen must be enabled on Windows 2012/2012 R2.	●	
▼ SRG-OS-000433-GPOS-00192	● 1	● 0

Explorer Data Execution Prevention must be enabled.	1	0
SRG-OS-000420-GPOS-00186	1	0
Turning off File Explorer heap termination on corruption must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
File Explorer shell protocol must run in protected mode.	1	0
SRG-OS-000095-GPOS-00049	1	0
The location feature must be turned off.	1	0
SRG-OS-000373-GPOS-00156	1	0
Passwords must not be saved in the Remote Desktop Client.	1	0
SRG-OS-000138-GPOS-00069	1	0
Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	1	0
SRG-OS-000373-GPOS-00156	1	0
Remote Desktop Services must always prompt a client for passwords upon connection.	1	0
SRG-OS-000033-GPOS-00014	1	0
Remote Desktop Services must be configured with the client connection encryption set to the required level.	1	0
SRG-OS-000480-GPOS-00227	1	0
Remote Desktop Services must delete temporary folders when a session is terminated.	1	0
Remote Desktop Services must be configured to use session-specific temporary folders.	1	0
Attachments must be prevented from being downloaded from RSS feeds.	1	0
SRG-OS-000095-GPOS-00049	1	0
Basic authentication for RSS feeds over HTTP must be turned off.	1	0

▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Users must be prevented from changing installation options.	●	
▼	● 1	● 0
■ The Windows Installer Always install with elevated privileges option must be disabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must be notified if a web-based program attempts to install software.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Nonadministrators must be prevented from applying vendor-signed updates.	●	
▼ SRG-OS-000095-GPOS-00049	● 1	● 0
■ Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Users must not be presented with Privacy and Installation options on first use of Windows Media Player.	●	
▼ SRG-OS-000362-GPOS-00149	● 1	● 0
■ Windows Media Player must be configured to prevent automatic checking for updates.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0
■ The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	●	
▼ SRG-OS-000125-GPOS-00065	● 1	● 0
■ The Windows Remote Management (WinRM) client must not use Digest authentication.	●	
▼	● 1	● 0
■ The Windows Remote Management (WinRM) service must not use Basic authentication.	●	
▼ SRG-OS-000393-GPOS-00173	● 1	● 0

<input type="checkbox"/> The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	●	
▼ SRG-OS-000373-GPOS-00156	● 1	● 0
<input type="checkbox"/> The Windows Remote Management (WinRM) service must not store RunAs credentials.	●	
▼ SRG-OS-000250-GPOS-00093	● 1	● 0
<input type="checkbox"/> The Remote Desktop Session Host must require secure RPC communications.	●	
▼ SRG-OS-000297-GPOS-00115	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	●	
▼	● 1	● 0
<input type="checkbox"/> Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	●	
▼ SRG-OS-000042-GPOS-00020	● 1	● 0
<input type="checkbox"/> Windows 2012 R2 must include command line data in process creation events.	●	
▼ SRG-OS-000191-GPOS-00080	● 1	● 0
<input type="checkbox"/> Systems must be maintained at a supported service pack level.	●	
▼	● 0	● 1
<input type="checkbox"/> The HBSS McAfee Agent must be installed.		●
▼ SRG-OS-000066-GPOS-00034	● 1	● 0
<input type="checkbox"/> The DoD Root CA certificates must be installed in the Trusted Root Store.	●	
▼	● 1	● 0

<input type="checkbox"/> The DoD Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
<input type="checkbox"/> The US DoD CCEB Interoperability Root CA cross-certificates must be installed into the Untrusted Certificates Store on unclassified systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Winlogon registry key.	● 1	● 0
<input type="checkbox"/> Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	● 1	● 0
▼ SRG-OS-000134-GPOS-00068	● 1	● 0
<input type="checkbox"/> Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	● 1	● 0
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
<input type="checkbox"/> Anonymous access to the registry must be restricted.	● 1	● 0
▼ SRG-OS-000121-GPOS-00062	● 1	● 0
<input type="checkbox"/> The built-in guest account must be disabled.	● 1	● 0
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Local accounts with blank passwords must be restricted to prevent access from the network.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in administrator account must be renamed.	● 1	● 0
▼	● 1	● 0
<input type="checkbox"/> The built-in guest account must be renamed.	● 1	● 0
▼ SRG-OS-000142-GPOS-00071	● 1	● 0
<input type="checkbox"/> Auditing the Access of Global System Objects must be turned off.	● 1	● 0
▼	● 1	● 0

<input type="checkbox"/> Auditing of Backup and Restore Privileges must be turned off.	●	
▼ SRG-OS-000062-GPOS-00031	● 1	● 0
<input type="checkbox"/> Audit policy using subcategories must be enabled.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> Ejection of removable NTFS media must be restricted to Administrators.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted or signed.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be encrypted when possible.	●	
▼	● 1	● 0
<input type="checkbox"/> Outgoing secure channel traffic must be signed when possible.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The computer account password must not be prevented from being reset.	●	
▼	● 1	● 0
<input type="checkbox"/> The maximum age for machine account passwords must be set to requirements.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
<input type="checkbox"/> The system must be configured to require a strong session key.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
<input type="checkbox"/> The system must be configured to prevent the display of the last username on the logon screen.	●	
▼	● 1	● 0
<input type="checkbox"/> The Ctrl+Alt+Del security attention sequence for logons must be enabled.	●	
▼ SRG-OS-000029-GPOS-00010	● 1	● 0
<input type="checkbox"/> The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	●	

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ Caching of logon credentials must be limited.	●	
▼	● 1	● 0
■ Users must be warned in advance of their passwords expiring.	●	
▼	● 1	● 0
■ The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB client must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB client must be enabled to perform SMB packet signing when possible.	●	
▼ SRG-OS-000074-GPOS-00042	● 1	● 0
■ Unencrypted passwords must not be sent to third-party SMB Servers.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The amount of idle time required before suspending a session must be properly set.	●	
▼ SRG-OS-000423-GPOS-00187	● 1	● 0
■ The Windows SMB server must be configured to always perform SMB packet signing.	●	
▼	● 1	● 0
■ The Windows SMB server must perform SMB packet signing when possible.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ Users must be forcibly disconnected when their logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The service principal name (SPN) target name validation level must be turned off.	●	
▼ SRG-OS-000480-GPOS-00229	● 1	● 0

Automatic logons must be disabled.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPv6 source routing must be configured to the highest protection level.	1	0
The system must be configured to prevent IP source routing.	1	0
The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to limit how often keep-alive packets are sent.	1	0
SRG-OS-000480-GPOS-00227	1	0
IPSec Exemptions must be limited.	1	0
SRG-OS-000420-GPOS-00186	1	0
The system must be configured to ignore NetBIOS name release requests except from WINS servers.	1	0
The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	1	0
SRG-OS-000480-GPOS-00227	1	0
The system must be configured to use Safe DLL Search Mode.	1	0
The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	1	0
SRG-OS-000420-GPOS-00186	1	0
IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	1	0

<input checked="" type="checkbox"/> The system must limit how many times unacknowledged TCP data is retransmitted.	1	0
▼ SRG-OS-000046-GPOS-00022	1	0
<input checked="" type="checkbox"/> The system must generate an audit event when the audit log reaches a percentage of full threshold.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of SAM accounts must not be allowed.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Anonymous enumeration of shares must be restricted.	1	0
▼ SRG-OS-000480-GPOS-00227	1	0
<input checked="" type="checkbox"/> The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	1	0
▼ SRG-OS-000138-GPOS-00069	1	0
<input checked="" type="checkbox"/> Named pipes that can be accessed anonymously must be configured to contain no values on member servers.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Unauthorized remotely accessible registry paths and sub-paths must not be configured.	1	0
▼	1	0
<input checked="" type="checkbox"/> Anonymous access to Named Pipes and Shares must be restricted.	1	0
▼	1	0
<input checked="" type="checkbox"/> Network shares that can be accessed anonymously must not be allowed.	1	0
▼	1	0
<input checked="" type="checkbox"/> The system must be configured to use the Classic security model.	1	0
▼ SRG-OS-000114-GPOS-00059	1	0
<input checked="" type="checkbox"/> Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	1	0

▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ NTLM must be prevented from falling back to a Null session.	●	
▼	● 1	● 0
■ PKU2U authentication using online identities must be prevented.	●	
▼ SRG-OS-000120-GPOS-00061	● 0	● 1
■ Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.		●
▼ SRG-OS-000073-GPOS-00041	● 1	● 0
■ The system must be configured to prevent the storage of the LAN Manager hash of passwords.	●	
▼ SRG-OS-000163-GPOS-00072	● 1	● 0
■ The system must be configured to force users to log off when their allowed logon hours expire.	●	
▼ SRG-OS-000480-GPOS-00227	● 1	● 0
■ The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.	●	
▼	● 1	● 0
■ The system must be configured to the required LDAP client signing level.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	●	
▼	● 1	● 0
■ The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	●	
▼	● 1	● 0
■ The shutdown option must not be available from the logon dialog box.	●	
▼ SRG-OS-000396-GPOS-00176	● 0	● 1
■ The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.		●
▼ SRG-OS-000480-GPOS-00227	● 1	● 0

<input checked="" type="checkbox"/> The system must be configured to require case insensitivity for non-Windows subsystems.	1	0
<input checked="" type="checkbox"/> The default permissions of global system objects must be increased.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control approval mode for the built-in Administrator must be enabled.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must, at minimum, prompt administrators for consent.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must automatically deny standard user requests for elevation.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must be configured to detect application installations and prompt for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> Windows must elevate all applications in User Account Control, not just signed ones.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must only elevate UIAccess applications that are installed in secure locations.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	1	0
SRG-OS-000134-GPOS-00068	1	0
<input checked="" type="checkbox"/> User Account Control must switch to the secure desktop when prompting for elevation.	1	0
SRG-OS-000373-GPOS-00157	1	0
<input checked="" type="checkbox"/> User Account Control must virtualize file and registry write failures to per-user locations.	1	0
SRG-OS-000134-GPOS-00068	1	0

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	1	0
SRG-OS-000095-GPOS-00049	1	0
Optional Subsystems must not be permitted to operate on the system.	1	0
SRG-OS-000362-GPOS-00149	1	0
The print driver installation privilege must be restricted to administrators.	1	0
SRG-OS-000067-GPOS-00035	1	0
Users must be required to enter a password to access private keys stored on the computer.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Fax service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Microsoft FTP service must not be installed unless required.	1	0
SRG-OS-000095-GPOS-00049	1	0
The Peer Networking Identity Manager service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Simple TCP/IP Services service must be disabled if installed.	1	0
SRG-OS-000096-GPOS-00050	1	0
The Telnet service must be disabled if installed.	1	0
SRG-OS-000480-GPOS-00227	1	0
The Smart Card Removal Policy service must be configured to automatic.	1	0
SRG-OS-000324-GPOS-00125	1	0
The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	1	0
SRG-OS-000080-GPOS-00048	1	0
The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	1	0

▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Act as part of the operating system user right must not be assigned to any groups or accounts.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0
■ The Allow log on locally user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group and other approved groups.	●	
▼ SRG-OS-000324-GPOS-00125	● 1	● 0
■ The Back up files and directories user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a pagefile user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Create a token object user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	●	
▼	● 1	● 0
■ The Create permanent shared objects user right must not be assigned to any groups or accounts.	●	
▼	● 1	● 0
■ The Create symbolic links user right must only be assigned to the Administrators group.	●	
▼	● 1	● 0
■ The Debug programs user right must only be assigned to the Administrators group.	●	
▼ SRG-OS-000080-GPOS-00048	● 1	● 0

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.



1

0

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems.



1

0

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems, and from unauthenticated access on all systems.



1

0

SRG-OS-000324-GPOS-00125

Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on member servers.



1

0

The Force shutdown from a remote system user right must only be assigned to the Administrators group.



1

0

The Generate security audits user right must only be assigned to Local Service and Network Service.



1

0

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.



1

0

The Increase scheduling priority user right must only be assigned to the Administrators group.



	 1  0
 The Load and unload device drivers user right must only be assigned to the Administrators group.	
	 1  0
 The Lock pages in memory user right must not be assigned to any groups or accounts.	
	 1  0
 The Manage auditing and security log user right must only be assigned to the Administrators group.	
	 1  0
 The Modify firmware environment values user right must only be assigned to the Administrators group.	
	 1  0
 The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	 1  0
 The Profile single process user right must only be assigned to the Administrators group.	
	 1  0
 The Restore files and directories user right must only be assigned to the Administrators group.	
	 1  0
 The Take ownership of files or other objects user right must only be assigned to the Administrators group.	