Windows Security Benchmark [6.0.0.0]

CSDEMO-DC01

Company Confidential

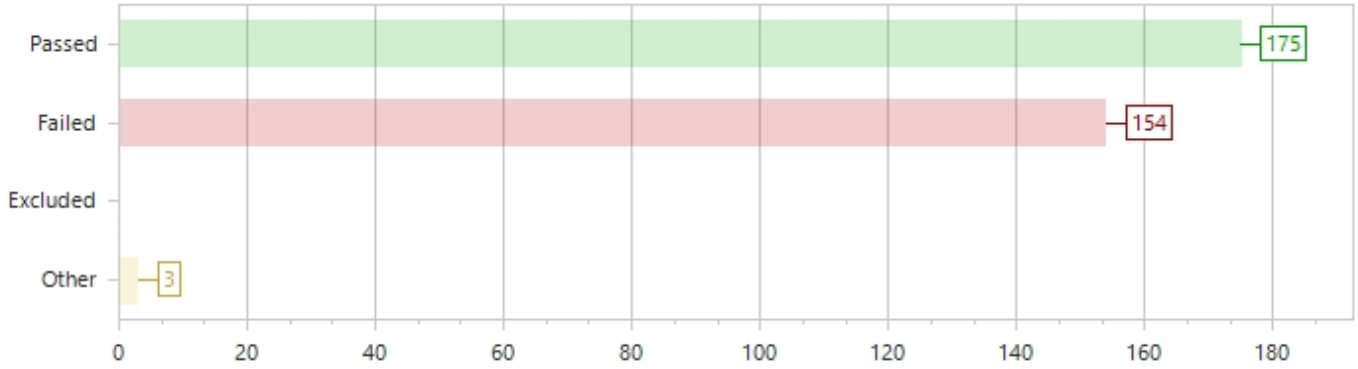
Document Properties

Author	CENTREL-WS01\XiaAdmin
Product	XIA Configuration Server [18.1.6.0]
Date	Wednesday, September 16, 2026 1:30:41 PM
Version	1.08

Table of Contents

Windows Security Benchmark [6.0.0.0]

The Windows Security Benchmark evaluates the security configuration of Windows operating systems, including both physical and virtual servers and workstations. It provides a consistent baseline for assessing and comparing security related policies, audit controls, account settings, and system configuration. The benchmark automatically adapts to the role of each machine - workstation, server, or domain controller to ensure accurate and relevant compliance results across diverse Windows environments.



Section 1: Password Policy

The checks in this section verify that the machine enforces a strong Windows password policy designed to prevent weak, guessable, or reused credentials. These controls ensure that password creation, storage, and lifecycle rules meet modern security expectations for both standalone and domain-joined Windows systems.

These checks align with industry recommendations such as Microsoft's Windows password policy guidance.

7 Benchmark Results

Ref.	Result	Title	Configured Value
1.01	Passed	Set "Enforce password history" to remember at least 24 passwords	24
1.02	Passed	Set "Maximum password age" to 60 days or less	42 days
1.03	Passed	Set "Minimum password age" to at least 1 day(s)	1 days
1.04	Failed	Set "Minimum password length" to 14 or more characters	7
1.05	Passed	Set "Password must meet complexity requirements" to "Enabled"	Enabled
1.06	Passed	Set "Store passwords using reversible encryption" to "Disabled"	False
1.07	Failed	Set "Relax minimum password length limits" to "Enabled" on supported operating systems	Not Configured

Section 2: Account Lockout Policy

The checks in this section verify that the machine enforces a secure Windows account lockout policy designed to limit repeated authentication failures and reduce the risk of brute-force attacks. These controls ensure that lockout thresholds, durations, and reset timers are configured to balance security with usability for both standalone and domain-joined Windows systems.

These checks align with industry recommendations such as Microsoft's Windows account lockout policy guidance.

3 Benchmark Results

Ref.	Result	Title	Configured Value
2.01	Failed	Set the "Account lockout duration" to 30 minutes or longer	Not Applicable
2.02	Failed	Set the "Account lockout threshold" to greater than 4 and less than 10	0
2.03	Failed	Set the "Reset account lockout counter after" value to between 15 minutes and 30 minutes	Not Applicable

Section 3: Windows Remote Management (WinRM)

The checks in this section verify that Windows Remote Management is configured securely to prevent credential exposure, downgrade attacks, and unauthenticated access. These controls ensure that both the WinRM client and service enforce encrypted communication, reject weak authentication methods, and avoid storing sensitive RunAs credentials, while still allowing secure remote shell access where required.

7 Benchmark Results

Ref.	Result	Title	Configured Value
3.01	Failed	Set "Allow Basic Authentication" to "False" for the WinRM Client	True
3.02	Failed	Set "Allow Digest Authentication" to "False" for the WinRM Client	True
3.03	Passed	Set "Allow Unencrypted Traffic" to "False" for the WinRM Client	False
3.04	Passed	Set "Allow Basic Authentication" to "False" for the WinRM Service	False
3.05	Passed	Set "Allow Unencrypted Traffic" to "False" for the WinRM Service	False
3.06	Failed	Set "Disallow Storing RunAs Credentials" to "True" for the WinRM Service	False
3.07	Passed	Set "Allow Remote Shell Access" to "True" for the Windows Remote Shell	True

Section 5: Server Functions

The checks in this section verify that the machine is not performing multiple conflicting server roles and is dedicated to a single primary function. These controls ensure that hosts are deployed with clear role separation, reducing the attack surface, simplifying security hardening, and preventing unintended privilege interactions between unrelated services.

1 Benchmark Results

Ref.	Result	Title	Configured Value
5.01	Failed	Limit the number of server functions to one per server	DNS Server Domain Controller

Section 6: Remote Desktop Settings

The checks in this section verify that Remote Desktop Services are configured securely to prevent unauthorized remote access, session hijacking, and data leakage through redirected devices. These controls ensure that only secure connection modes are permitted, strong encryption is enforced, credential prompts are required, and redirection of drives, ports, and plug-and-play devices is disabled to reduce the attack surface of remote sessions.

12 Benchmark Results

Ref.	Result	Title	Configured Value
6.01	Passed	Set "Connection Mode" to "Don't allow remote connections" or "Only allow connections with network level authentication (more secure)"	Don't allow remote connections
6.02	Passed	Set "Disable COM Port Redirection" to "True"	Don't allow remote connections
6.03	Passed	Set "Disable Drive Redirection" to "True"	Don't allow remote connections
6.04	Passed	Set "Disable LPT Port Redirection" to "True"	Don't allow remote connections
6.05	Passed	Set "Disable Plug and Play Device" to "True"	Don't allow remote connections
6.06	Passed	Set "Always Prompt For Password" to "True"	Don't allow remote connections
6.07	Passed	Set "Security Layer" to "SSL"	Don't allow remote connections
6.08	Passed	Set "Minimum Encryption Level" to "High"	Don't allow remote connections
6.09	Passed	Set "Single Session Restriction" to "True"	Don't allow remote connections
6.10	Passed	Set "Use Temporary Folders Per Session" to "True"	Don't allow remote connections
6.11	Passed	Set "Delete Temporary Folders On Exit" to "True"	Don't allow remote connections
6.12	Passed	Set "Require Secure RPC Communication" to "True"	Don't allow remote connections

Section 7: Audit Settings

The checks in this section verify that Windows audit policy and advanced audit policy subcategories are configured to provide comprehensive, reliable security logging across the system. These controls ensure that authentication events, account management activity, policy changes, object access, privilege use, and system integrity events are captured consistently, enabling effective monitoring, incident investigation, and compliance reporting.

These checks align with industry recommendations such as Microsoft's Audit Policy Recommendations.

61 Benchmark Results

Ref.	Result	Title	Configured Value
7.01	Passed	Set "Audit: Audit the access of global system objects" to "Disabled"	Disabled
7.02	Passed	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Disabled
7.03	Failed	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Not Defined
7.04	Failed	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Success
7.05	Failed	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Success
7.06	Failed	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Success
7.07	Failed	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	None
7.08	Passed	Set the "Audit Application Group Management" advanced audit policy to "None"	None
7.09	Failed	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Success
7.10	Passed	Set the "Audit Distribution Group Management" advanced audit policy to "None"	None
7.11	Failed	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	None
7.12	Failed	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Success

7.13	Failed	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Success
7.14	Failed	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	None
7.15	Passed	Set the "Audit PNP Activity" advanced audit policy to "Any"	None
7.16	Failed	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	None
7.17	Passed	Set the "Audit Process Termination" advanced audit policy to "None"	None
7.18	Passed	Set the "Audit RPC Events" advanced audit policy to "None"	None
7.19	Passed	Set the "Audit Detailed Directory Service Replication" advanced audit policy to "None" on domain controllers	None
7.20	Passed	Set the "Audit Directory Service Access" advanced audit policy to "None" on domain controllers	Success
7.21	Passed	Set the "Audit Directory Service Changes" advanced audit policy to "None" on domain controllers	None
7.22	Passed	Set the "Audit Directory Service Replication" advanced audit policy to "None" on domain controllers	None
7.23	Passed	Set the "Audit Account Lockout" advanced audit policy to "Success"	Success
7.24	Failed	Set the "Audit Group Membership" advanced audit policy to "Success"	None
7.25	Passed	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	None
7.26	Passed	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	None
7.27	Passed	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	None
7.28	Passed	Set the "Audit Logoff" advanced audit policy to "Success"	Success
7.29	Passed	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Success and Failure
7.30	Passed	Set the "Audit Network Policy Server" advanced audit policy to "None"	Success and Failure
7.31	Passed	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	None
7.32	Failed	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Success
7.33	Passed	Set the "Audit User/Device Claims" advanced audit policy to "None"	None

7.34	Passed	Set the "Audit Application Generated" advanced audit policy to "None"	None
7.35	Passed	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	None
7.36	Passed	Set the "Audit Certification Services" advanced audit policy to "None"	None
7.37	Passed	Set the "Audit Detailed File Share" advanced audit policy to "None"	None
7.38	Passed	Set the "Audit File Share" advanced audit policy to "None"	None
7.39	Passed	Set the "Audit File System" advanced audit policy to "None"	None
7.40	Passed	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	None
7.41	Passed	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	None
7.42	Passed	Set the "Audit Handle Manipulation" advanced audit policy to "None"	None
7.43	Passed	Set the "Audit Kernel Object" advanced audit policy to "None"	None
7.44	Passed	Set the "Audit Other Object Access Events" advanced audit policy to "None"	None
7.45	Passed	Set the "Audit Registry" advanced audit policy to "None"	None
7.46	Passed	Set the "Audit Removable Storage" advanced audit policy to "None"	None
7.47	Passed	Set the "Audit SAM" advanced audit policy to "None"	None
7.48	Failed	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Success
7.49	Failed	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Success
7.50	Passed	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	None
7.51	Passed	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	None
7.52	Failed	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	None
7.53	Passed	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	None
7.54	Passed	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	None

7.55	Passed	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	None
7.56	Passed	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	None
7.57	Failed	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	None
7.58	Passed	Set the "Audit Other System Events" advanced audit policy to "None"	Success and Failure
7.59	Failed	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Success
7.60	Failed	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	None
7.61	Passed	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Success and Failure

Section 8: Windows Update

The checks in this section verify that the machine is configured to receive and install security updates reliably through Windows Update or a managed update service such as WSUS. These controls ensure that the operating system remains protected against known vulnerabilities by enforcing automatic update installation and, where required, centralized update management.

These checks align with industry recommendations such as Microsoft's Windows Update configuration guidance.

2 Benchmark Results

Ref.	Result	Title	Configured Value
8.01	Passed	Enable Windows Update to receive updates	Download updates but let me choose whether to install them
8.02	Failed	Configure Windows Update to use Windows Server Update Services (WSUS)	

Section 9: Windows Time

The checks in this section verify that the Windows Time service is configured correctly to provide reliable and secure time synchronization across the environment. These controls ensure that all machines run the Windows Time client, domain members follow the domain hierarchy for time, and only domain controllers operate as NTP servers, preventing clock drift that can break authentication, Kerberos, logging, and security monitoring.

3 Benchmark Results

Ref.	Result	Title	Configured Value
9.01	Passed	Enable the Windows Time client on all machines	True
9.02	Failed	Set the NTP client type to "Domain Hierarchy (NT5DS)" for domain members and "NTP" for PDC emulators and machines on workgroups	Domain Hierarchy (NT5DS)
9.03	Passed	Enable the NTP server for domain controllers, and disable for all other servers and workstations	True

Section 10: SNMP

The checks in this section verify that Simple Network Management Protocol (SNMP), if enabled, is configured securely to prevent unauthorized access or disclosure of system information. These controls ensure that default community strings such as public and private are not used, and that no writable community strings are configured, reducing the risk of remote manipulation or information leakage.

2 Benchmark Results

Ref.	Result	Title	Configured Value
10.01	Passed	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Not Installed
10.02	Passed	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Not Installed

Section 11: Deprecated Components and Protocols

The checks in this section verify that legacy and insecure Windows components, specifically SMB version 1, are fully disabled on both the server and client. These controls ensure that outdated protocols are not available for use, reducing exposure to well-known vulnerabilities, preventing downgrade attacks, and aligning the system with modern Windows security standards.

2 Benchmark Results

Ref.	Result	Title	Configured Value
11.01	Passed	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Server Feature Disabled
11.02	Passed	Ensure that Server Message Block (SMB) version 1 is disabled for the client	Disabled

Section 12: Windows Event Log

The checks in this section verify that Windows Event Logs are configured with appropriate maximum sizes and retention policies to ensure reliable auditing, troubleshooting, and long-term security visibility. Larger log sizes prevent important events from being overwritten prematurely, while the correct retention mode ensures logs continue to capture new activity without manual intervention.

8 Benchmark Results

Ref.	Result	Title	Configured Value
12.01	Failed	Set the maximum size of the Application event log to 40,960 KB or greater	20,480 KB
12.02	Passed	Set the maximum size of the Security event log to 81,920 KB or greater	131,072 KB
12.03	Failed	Set the maximum size of the Setup event log to 20,480 KB or greater	1,028 KB
12.04	Passed	Set the maximum size of the System event log to 20,480 KB or greater	20,480 KB
12.05	Passed	Set the retention policy of the Application event log to 'Overwrite events as needed'	Overwrite events as needed
12.06	Passed	Set the retention policy of the Security event log to 'Overwrite events as needed'	Overwrite events as needed
12.07	Passed	Set the retention policy of the Setup event log to 'Overwrite events as needed'	Overwrite events as needed
12.08	Passed	Set the retention policy of the System event log to 'Overwrite events as needed'	Overwrite events as needed

Section 13: User Rights Assignment

The checks in this section verify that Windows User Rights Assignment is configured according to least-privilege principles. These rights determine which accounts can perform sensitive system-level operations such as logging on, accessing the system over the network, impersonation, debugging, backup/restore, and service execution. Correct configuration is essential for preventing privilege escalation, unauthorized access, and lateral movement.

These checks align with industry recommendations such as Microsoft's Windows User Rights Assignments guidance.

45 Benchmark Results

Ref.	Result	Title	Configured Value
13.01	Passed	Set the "Access Credential Manager as a trusted caller" user right to [Empty]	
13.02	Failed	Set the "Access this computer from the network" user right to include only [ENTERPRISE_DOMAIN_CONTROLLERS] BUILTIN\Administrators NT AUTHORITY\Authenticated Users	BUILTIN\Administrators BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
13.03	Passed	Set the "Act as part of the operating system" user right to [Empty]	
13.04	Failed	Set the "Add workstations to domain" user right to include only BUILTIN\Administrators on domain controllers	NT AUTHORITY\Authenticated Users
13.05	Passed	Set the "Adjust memory quotas for a process" user right to include only BUILTIN\Administrators IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL% NT SERVICE\SQLAgent% NT SERVICE\SQLSERVERAGENT	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

13.06	Failed	Set the "Allow log on locally" user right to include only BUILTIN\Account Operators BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators	BUILTIN\Account Operators BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
13.07	Passed	Set the "Allow log on through Remote Desktop Services" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.08	Passed	Set the "Back up files and directories" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
13.09	Passed	Set the "Bypass traverse checking" user right to [Any Value]	BUILTIN\Administrators BUILTIN\Pre-Windows 2000 Compatible Access Everyone NT AUTHORITY\Authenticated Users NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
13.10	Passed	Set the "Change the system time" user right to include only BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
13.11	Passed	Set the "Change the time zone" user right to [Any Value]	BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE
13.12	Passed	Set the "Create a pagefile" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.13	Passed	Set the "Create a token object" user right to [Empty]	
13.14	Passed	Set the "Create global objects" user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

		NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	NT AUTHORITY\SERVICE
13.15	Passed	Set the "Create permanent shared objects" user right to [Empty]	
13.16	Passed	Set the "Create symbolic links" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.17	Passed	Set the "Debug programs" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.18	Failed	Set the "Deny access to this computer from the network" user right to must include BUILTIN\Guests	
13.19	Failed	Set the "Deny log on as a batch job" user right to must include BUILTIN\Guests	
13.20	Failed	Set the "Deny log on as a service" user right to must include BUILTIN\Guests	
13.21	Failed	Set the "Deny log on locally" user right to must include BUILTIN\Guests	
13.22	Failed	Set the "Deny log on through Remote Desktop Services" user right to must include BUILTIN\Guests	
13.23	Passed	Set the "Enable computer and user accounts to be trusted for delegation" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.24	Failed	Set the "Force shutdown from a remote system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Server Operators
13.25	Failed	Set the "Generate security audits" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\adfssrv NT SERVICE\drs	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE RESTRICTED SERVICES\PrintSpoolerService
13.26	Failed	Set the "Impersonate a client after authentication" user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE

		NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	NT AUTHORITY\SERVICE RESTRICTED SERVICES\PrintSpoolerService
13.27	Passed	Set the "Increase a process working set" user right to include only BUILTIN\Users S-1-5-32-583 Window Manager\Window Manager Group	BUILTIN\Users
13.28	Passed	Set the "Increase scheduling priority" user right to include only BUILTIN\Administrators Window Manager\Window Manager Group	BUILTIN\Administrators Window Manager\Window Manager Group
13.29	Failed	Set the "Load and unload device drivers" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Print Operators
13.30	Passed	Set the "Lock pages in memory" user right to [Empty]	
13.31	Passed	Set the "Log on as a batch job" user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\IIS_IUSRS BUILTIN\Performance Log Users	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Performance Log Users
13.32	Failed	Set the "Log on as a service" user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	CSDEMO\Administrator CSDEMO\pGMSA_c2ca7496$ CSDEMO\XiaClient NT SERVICE\ALL SERVICES NT SERVICE\himds RESTRICTED SERVICES\ALL RESTRICTED SERVICES
13.33	Failed	Set the "Manage auditing and security log" user right to include only BUILTIN\Administrators	BUILTIN\Administrators CSDEMO\Exchange Servers
13.34	Passed	Set the "Modify an object label" user right to [Empty]	
13.35	Passed	Set the "Modify firmware environment values" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.36	Unknown	Set the "Obtain an impersonation token for another user in the same session" user right to include only BUILTIN\Administrators	Unknown
13.37	Passed	Set the "Perform volume maintenance tasks" user right to include only	BUILTIN\Administrators

		BUILTIN\Administrators	
13.38	Passed	Set the "Profile single process" user right to include only BUILTIN\Administrators	BUILTIN\Administrators
13.39	Passed	Set the "Profile system performance" user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	BUILTIN\Administrators NT SERVICE\WdiServiceHost
13.40	Passed	Set the "Remove computer from docking station" user right to [Any Value]	BUILTIN\Administrators
13.41	Passed	Set the "Replace a process level token" user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE
13.42	Failed	Set the "Restore files and directories" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators
13.43	Failed	Set the "Shut down the system" user right to include only BUILTIN\Administrators	BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Print Operators BUILTIN\Server Operators
13.44	Passed	Set the "Synchronize directory service data" user right to [Empty]	
13.45	Passed	Set the "Take ownership of files or other objects" user right to include only BUILTIN\Administrators	BUILTIN\Administrators

Section 14: Windows Firewall Domain Profile

The checks in this section verify that the Windows Firewall Domain Profile is configured to enforce secure network boundaries when the system is connected to a domain network. The domain profile governs inbound and outbound traffic rules, logging behavior, and notification settings. Correct configuration ensures that only authorized traffic is permitted, security-relevant events are logged, and administrators receive appropriate visibility into firewall activity.

These checks align with industry recommendations such as Microsoft's Windows Firewall guidance.

9 Benchmark Results

Ref.	Result	Title	Configured Value
14.01	Passed	Set the Windows Firewall domain profile firewall state to "On (recommended)"	On (recommended)
14.02	Passed	Set the Windows Firewall domain profile default inbound action to "Block (default)"	Block (default)
14.03	Passed	Set the Windows Firewall domain profile default outbound action to "Allow (default)"	Allow (default)
14.04	Passed	Set the Windows Firewall domain profile display a notification setting to "No"	No
14.05	Passed	Set the Windows Firewall domain profile excluded network interfaces to none	
14.06	Failed	Set the Windows Firewall domain profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\DomainProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
14.07	Failed	Set the Windows Firewall domain profile log file size limit to 16,384 KB or greater	4,096 KB
14.08	Failed	Set the Windows Firewall domain profile log dropped packets setting to "Yes"	No
14.09	Failed	Set the Windows Firewall domain profile log successful connections setting to "Yes"	No

Section 15: Windows Firewall Private Profile

The checks in this section verify that the Windows Firewall Private Profile is configured to enforce secure network boundaries when the system is connected to a private network. The private profile governs inbound and outbound traffic rules, logging behavior, and notification settings. Correct configuration ensures that only authorized traffic is permitted, security-relevant events are logged, and administrators receive appropriate visibility into firewall activity.

These checks align with industry recommendations such as Microsoft's Windows Firewall guidance.

9 Benchmark Results

Ref.	Result	Title	Configured Value
15.01	Passed	Set the Windows Firewall private profile firewall state to "On (recommended)"	On (recommended)
15.02	Passed	Set the Windows Firewall private profile default inbound action to "Block (default)"	Block (default)
15.03	Passed	Set the Windows Firewall private profile default outbound action to "Allow (default)"	Allow (default)
15.04	Passed	Set the Windows Firewall private profile display a notification setting to "No"	No
15.05	Passed	Set the Windows Firewall private profile excluded network interfaces to none	
15.06	Failed	Set the Windows Firewall private profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PrivateProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
15.07	Failed	Set the Windows Firewall private profile log file size limit to 16,384 KB or greater	4,096 KB
15.08	Failed	Set the Windows Firewall private profile log dropped packets setting to "Yes"	No
15.09	Failed	Set the Windows Firewall private profile log successful connections setting to "Yes"	No

Section 16: Windows Firewall Public Profile

The checks in this section verify that the Windows Firewall Public Profile is configured to enforce secure network boundaries when the system is connected to a public network. The public profile governs inbound and outbound traffic rules, logging behavior, and notification settings. Correct configuration ensures that only authorized traffic is permitted, security-relevant events are logged, and administrators receive appropriate visibility into firewall activity.

These checks align with industry recommendations such as Microsoft's Windows Firewall guidance.

9 Benchmark Results

Ref.	Result	Title	Configured Value
16.01	Passed	Set the Windows Firewall public profile firewall state to "On (recommended)"	On (recommended)
16.02	Passed	Set the Windows Firewall public profile default inbound action to "Block (default)"	Block (default)
16.03	Passed	Set the Windows Firewall public profile default outbound action to "Allow (default)"	Allow (default)
16.04	Passed	Set the Windows Firewall public profile display a notification setting to "No"	No
16.05	Passed	Set the Windows Firewall public profile excluded network interfaces to none	
16.06	Failed	Set the Windows Firewall public profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PublicProfile.log"	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
16.07	Failed	Set the Windows Firewall public profile log file size limit to 16,384 KB or greater	4,096 KB
16.08	Failed	Set the Windows Firewall public profile log dropped packets setting to "Yes"	No
16.09	Failed	Set the Windows Firewall public profile log successful connections setting to "Yes"	No

Section 17: Security Options (General)

The checks in this section verify that general Windows Security Options are configured to enforce privacy controls, restrict consumer-grade cloud features, and harden device pairing, biometrics, and workspace behavior.

7 Benchmark Results

Ref.	Result	Title	Configured Value
17.01	Failed	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Not Defined
17.02	Failed	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Not Defined
17.03	Failed	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Not Defined
17.04	Failed	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Not Defined
17.05	Failed	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Not Defined
17.06	Failed	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Not Defined
17.07	Failed	Set the "Windows Ink Workspace: Allow Windows Ink Workspace" security option to "Disabled" or "On, but disallow access above lock"	Not Defined

Section 18: Security Options (Accounts)

The checks in this section verify that account-related Windows Security Options are configured to enforce strong authentication controls and prevent insecure login behavior. These policies help ensure that Microsoft consumer accounts cannot be added to enterprise systems.

2 Benchmark Results

Ref.	Result	Title	Configured Value
18.01	Failed	Set the "Accounts: Block Microsoft accounts" security option to "Users can’t add or log on with Microsoft accounts"	Not Defined
18.02	Passed	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Enabled

Section 19: Security Options (Audit)

The checks in this section verify that audit-related Windows Security Options are configured to ensure reliable event logging without introducing unnecessary operational risk.

2 Benchmark Results

Ref.	Result	Title	Configured Value
19.01	Passed	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Not Defined
19.02	Passed	Set the "Audit: Shut down system immediately if unable to log security audits" security option to "Disabled"	Disabled

Section 20: Security Options (Credential User Interface)

The checks in this section verify that the machine enforces secure Windows Credential User Interface settings designed to reduce credential exposure and prevent disclosure of privileged account information.

2 Benchmark Results

Ref.	Result	Title	Configured Value
20.01	Failed	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Not Defined
20.02	Failed	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Not Defined

Section 21: Security Options (Credentials Delegation)

The checks in this section verify that the machine enforces secure credential-delegation behavior to prevent downgrade attacks and ensure that only protected, non-exportable credentials can be delegated to remote hosts.

2 Benchmark Results

Ref.	Result	Title	Configured Value
21.01	Failed	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Not Defined
21.02	Failed	Set the "Credentials Delegation: Remote host allows delegation of non-exportable credentials" security option to "Enabled"	Not Defined

Section 22: Security Options (Data Collection and Preview Builds)

The checks in this section verify that the machine restricts Windows diagnostic data, feedback prompts, and Insider-build controls to prevent unnecessary telemetry and block users from enrolling devices into preview or experimental build channels.

3 Benchmark Results

Ref.	Result	Title	Configured Value
22.01	Failed	Set the "Data Collection and Preview Builds: Allow Diagnostics Data" security option to "Diagnostic data off (not recommended)" or "Send required diagnostic data" on Windows Server 2022, Windows 10 build 20348, Windows 11 and newer	Not Defined
22.03	Failed	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Not Defined
22.04	Failed	Set the "Data Collection and Preview Builds: Toggle user control over Insider builds" security option to "Disabled"	Not Defined

Section 23: Security Options (Devices)

The checks in this section verify that the machine restricts device-level actions that could expose data or weaken endpoint control.

2 Benchmark Results

Ref.	Result	Title	Configured Value
23.01	Failed	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Not Defined
23.02	Passed	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Enabled

Section 24: Security Options (Domain Controllers)

The checks in this section verify that the domain controller enforces strict security controls around task scheduling, LDAP signing, and machine account password management.

3 Benchmark Results

Ref.	Result	Title	Configured Value
24.01	Failed	Set the "Domain controller: Allow server operators to schedule tasks" security option to "Disabled" on domain controllers	Not Defined
24.02	Failed	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing" on domain controllers	None
24.03	Failed	Set the "Domain controller: Refuse machine account password changes" security option to "Disabled" on domain controllers	Not Defined

Section 25: Security Options (Domain Members)

The checks in this section verify that domain joined machines enforce secure channel protections, strong cryptographic requirements, and healthy machine account password hygiene.

6 Benchmark Results

Ref.	Result	Title	Configured Value
25.01	Passed	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Enabled
25.02	Passed	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled" on domain members	Enabled
25.03	Passed	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Enabled
25.04	Passed	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Disabled
25.05	Passed	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	30 days
25.06	Passed	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled" on domain members	Enabled

Section 26: Security Options (Explorer Shell)

The checks in this section verify that the machine enforces hardened Explorer shell behavior to reduce the risk of malware execution, unsafe removable media actions, and user exposure to untrusted content.

8 Benchmark Results

Ref.	Result	Title	Configured Value
26.01	Failed	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Not Defined
26.02	Failed	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Not Defined
26.03	Failed	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Not Defined
26.04	Failed	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Not Defined
26.05	Failed	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Not Defined
26.06	Failed	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Not Defined
26.07	Passed	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Not Defined
26.08	Passed	Set the "File Explorer: Turn off shell protocol protected mode" security option to "Disabled" or "Not Defined"	Not Defined

Section 27: Security Options (Group Policy)

The checks in this section verify that the machine applies Group Policy settings consistently and securely, ensuring that registry based policy changes are processed reliably and that user experience related continuation features are disabled on domain joined systems.

4 Benchmark Results

Ref.	Result	Title	Configured Value
27.01	Failed	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on domain members	Not Defined
27.02	Failed	Set the "Group Policy: Registry policy processing: Do not apply during periodic background processing" security option to "Disabled" on domain members	Not Defined
27.03	Failed	Set the "Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed" security option to "Enabled" on domain members	Not Defined
27.04	Passed	Set the "Group Policy: Turn off background refresh of Group Policy" security option to "Disabled" or "Not Defined" on domain members	Not Defined

Section 28: Security Options (Interactive Logon)

The checks in this section verify that the machine enforces secure and predictable interactive logon behavior, ensuring that users cannot glean unnecessary account information, that inactivity and lockout controls are in place, and that organizations can present mandatory legal or informational logon banners.

8 Benchmark Results

Ref.	Result	Title	Configured Value
28.01	Failed	Set the "Interactive logon: Don't display last signed-in" security option to "Enabled"	Disabled
28.02	Passed	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Disabled
28.03	Failed	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Not Defined
28.04	Failed	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Not Defined
28.05	Manual	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	
28.06	Manual	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	
28.08	Passed	Set the "Interactive logon: Prompt user to change password before expiration" security option to a value between 5 and 10 days	5 days
28.10	Failed	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation", "Force Logoff", or "Disconnect if a Remote Desktop Services session"	No Action

Section 29: Security Options (Internet Explorer - Deprecated)

The checks in this section verify that the machine fully disables legacy Internet Explorer behaviors and prevents users from launching the deprecated browser thereby reducing exposure to legacy web-based attacks.

2 Benchmark Results

Ref.	Result	Title	Configured Value
29.01	Failed	Set the "Internet Explorer: Disable Internet Explorer as a stand alone browser" security option to "Disable browser never notify user", "Disable browser always notify user", or "Disable browser notify user once"	Not Defined
29.02	Failed	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Not Defined

Section 30: Security Options (Lanman Workstation)

The checks in this section verify that the machine prevents insecure guest authentication over SMB, ensuring that Windows does not fall back to unauthenticated "guest" access when connecting to remote file shares.

1 Benchmark Results

Ref.	Result	Title	Configured Value
30.01	Failed	Set the "Lanman Workstation: Enable insecure guest logons" security option to "Disabled"	Not Defined

Section 31: Security Options (Logon)

The checks in this section verify that the machine restricts what information and notifications are visible on the Windows sign-in and lock screens.

7 Benchmark Results

Ref.	Result	Title	Configured Value
31.01	Failed	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Not Defined
31.02	Failed	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Not Defined
31.03	Failed	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Not Defined
31.05	Failed	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Not Defined
31.06	Failed	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Not Defined
31.07	Failed	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Not Defined
31.08	Passed	Set the "Windows Logon Options: Sign-in and lock last interactive user automatically after a restart" security setting to "Disabled"	Disabled

Section 32: Security Options (Microsoft Accounts)

The checks in this section verify that the machine blocks consumer Microsoft account authentication, ensuring that only organizational identities can be used for sign-in or elevation.

1 Benchmark Results

Ref.	Result	Title	Configured Value
32.01	Failed	Set the "Microsoft Accounts: Block all consumer Microsoft account user authentication" security option to "Enabled"	Not Defined

Section 33: Security Options (Microsoft Defender Antivirus)

The checks in this section verify that the machine enforces key Microsoft Defender Antivirus protections designed to block unwanted applications, prevent access to dangerous websites, and ensure that core scanning capabilities remain active.

9 Benchmark Results

Ref.	Result	Title	Configured Value
33.01	Failed	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Not Defined
33.02	Passed	Set the "Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
33.03	Failed	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Not Defined
33.04	Passed	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Not Defined
33.05	Failed	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Not Defined
33.06	Failed	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Not Defined
33.07	Passed	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Not Defined
33.08	Passed	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Not Defined
33.09	Failed	Set the "Microsoft Defender Antivirus: Turn on e-mail scanning" security option to "Enabled"	Not Defined

Section 34: Security Options (Microsoft Network Client)

The checks in this section verify that the machine enforces secure SMB client behavior by requiring digital signing and preventing the use of unencrypted passwords when connecting to third-party SMB servers.

3 Benchmark Results

Ref.	Result	Title	Configured Value
34.01	Failed	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Not Defined
34.02	Passed	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Enabled
34.03	Passed	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Disabled

Section 35: Security Options (Microsoft Network Server)

The checks in this section verify that the machine enforces secure SMB server behavior by requiring digital signing, validating SPN target names, and ensuring sessions are suspended or disconnected appropriately.

5 Benchmark Results

Ref.	Result	Title	Configured Value
35.01	Passed	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	15 minutes
35.02	Passed	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Enabled
35.03	Passed	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Enabled
35.04	Passed	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Enabled
35.05	Failed	Set the "Microsoft network server: Server SPN target name validation level" security option to "Accept if provided by client" or "Required from client"	Not Defined

Section 36: Security Options (MSS - Deprecated)

The checks in this section verify a collection of legacy "MSS" (Microsoft Security Settings) options that harden older networking, routing, and system behavior features still present for backward compatibility. Although deprecated, these controls remain relevant for reducing spoofing risks, preventing unsafe routing behaviors, tightening TCP retransmission limits, enforcing Safe DLL search mode, and ensuring timely screen-lock grace periods.

12 Benchmark Results

Ref.	Result	Title	Configured Value
36.01	Passed	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Not Defined
36.02	Failed	Set the "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
36.03	Failed	Set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Not Defined
36.04	Failed	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Enabled
36.05	Failed	Set the "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds" security option to "300000 or 5 minutes (recommended)"	Not Defined
36.06	Failed	Set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" security option to "Enabled"	Not Defined
36.07	Failed	Set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" security option to "Disabled"	Not Defined
36.08	Passed	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Not Defined
36.09	Failed	Set the "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)" security option to 5 seconds or less	Not Defined
36.10	Failed	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Not Defined

⊗ 36.11	Failed	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Not Defined
⊗ 36.12	Failed	Set the "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning" security option to 90% or less	Not Defined

Section 37: Security Options (Network)

The checks in this section verify that the machine disables insecure name resolution mechanisms and avoids legacy NetBIOS broadcast behavior.

2 Benchmark Results

Ref.	Result	Title	Configured Value
37.01	Failed	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Not Defined
37.02	Failed	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Not Defined

Section 38: Security Options (Network Access)

The checks in this section verify that the machine restricts anonymous access to sensitive network resources, prevents credential storage for network authentication, and tightly controls which registry paths, shares, and named pipes can be accessed remotely.

11 Benchmark Results

Ref.	Result	Title	Configured Value
38.01	Passed	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Disabled
38.02	Failed	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Disabled
38.03	Passed	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Enabled
38.04	Failed	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Disabled
38.05	Passed	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Disabled
38.06	Failed	Set the "Network access: Named Pipes that can be accessed anonymously" security option to only contain [Empty]	netlogon samr lsarpc
38.07	Passed	Set the "Network access: Remotely accessible registry paths and subpaths" security option to include only Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog	Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Perflib Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration

		System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Services\Eventlog System\CurrentControlSet\Services\SysmonLog
38.08	Passed	Set the "Network access: Remotely accessible registry paths" security option to include only Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications	Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications
38.09	Passed	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Enabled
38.11	Failed	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Not Defined
38.12	Passed	Set the "Network access: Sharing and security model for local accounts" security option to "Classic - Local users authenticate as themselves"	Classic - local users authenticate as themselves

Section 39: Security Options (Network Connections)

The checks in this section verify that the machine prevents users from configuring network bridging features, blocks Internet Connection Sharing, and requires elevation when domain users attempt to change a network's location.

3 Benchmark Results

Ref.	Result	Title	Configured Value
39.01	Failed	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Not Defined
39.02	Failed	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Not Defined
39.03	Failed	Set the "Network Connections: Require domain users to elevate when setting a network's location" security option to "Enabled"	Not Defined

Section 40: Security Options (Network Provider)

The checks in this section verify that the machine enforces Hardened UNC Paths, ensuring that access to critical domain resources, specifically NETLOGON and SYSVOL, requires both mutual authentication and integrity protection.

1 Benchmark Results

Ref.	Result	Title	Configured Value
40.01	Passed	Set the "Network Provider: Hardened UNC Paths" security option to *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1	

Section 41: Security Options (Network Security)

The checks in this section verify that the machine enforces modern, hardened authentication and session security requirements across NTLM, LDAP, and secure RPC.

10 Benchmark Results

Ref.	Result	Title	Configured Value
41.01	Failed	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Not Defined
41.02	Failed	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Not Defined
41.03	Failed	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" on domain members	Not Defined
41.04	Failed	Set the "Network security: Configure encryption types allowed for Kerberos" security option to "AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types" on domain members	Not Defined
41.05	Passed	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Enabled
41.06	Failed	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Disabled
41.07	Failed	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Not Defined
41.08	Failed	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Negotiate Signing
41.09	Failed	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption
41.10	Failed	Set the "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" security option to "Require NTLMv2 session security, Require 128-bit encryption"	Require 128-bit encryption

Section 42: Security Options (Personalization)

The checks in this section verify that the machine prevents users from enabling potentially distracting or privacy reducing lock screen features.

2 Benchmark Results

Ref.	Result	Title	Configured Value
42.01	Failed	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Not Defined
42.02	Failed	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Not Defined

Section 43: Security Options (Recovery Console)

The checks in this section verify that the machine restricts potentially unsafe Recovery Console behaviors by disabling automatic administrative logon and blocking access to drives, folders, and removable media during recovery operations.

2 Benchmark Results

Ref.	Result	Title	Configured Value
43.01	Passed	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Disabled
43.02	Passed	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Disabled

Section 44: Security Options (Remote Assistance)

The checks in this section verify that the machine prevents both Offer and Solicited Remote Assistance, ensuring that no user or administrator can initiate or request Remote Assistance sessions.

2 Benchmark Results

Ref.	Result	Title	Configured Value
44.01	Failed	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Not Defined
44.02	Failed	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Not Defined

Section 45: Security Options (Remote Desktop Connection Client)

The check in this section verifies that the machine prevents Remote Desktop Connection Client from saving passwords. Enforcing this control ensures that RDP credentials are never stored locally, reducing the risk of credential theft, lateral movement, and unauthorized reuse of cached passwords.

1 Benchmark Results

Ref.	Result	Title	Configured Value
45.01	Failed	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Not Defined

Section 47: Security Options (Search)

The checks in this section verify that the machine restricts cloud based search integration and prevents indexing of encrypted files.

2 Benchmark Results

Ref.	Result	Title	Configured Value
47.01	Failed	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Not Defined
47.02	Passed	Set the "Search: Allow indexing of encrypted files" security option to "Disabled" or "Not Defined"	Not Defined

Section 48: Security Options (Security Providers)

The checks in this section verify that the system enforces secure authentication provider behavior by disabling legacy or vulnerable mechanisms such as WDigest.

1 Benchmark Results

Ref.	Result	Title	Configured Value
48.01	Passed	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Not Defined

Section 49: Security Options (Startup and Shutdown)

The checks in this section verify that the system enforces secure behavior during startup and shutdown by controlling early-boot antimalware policy, restricting unauthenticated shutdown actions, and ensuring sensitive memory is cleared when the machine powers off.

3 Benchmark Results

Ref.	Result	Title	Configured Value
49.01	Passed	Set the "Early Launch Antimalware: Boot-Start Driver Initialization Policy" security option to "Good, unknown and bad but critical" or "Not Defined"	Not Defined
49.02	Passed	Set the "Shutdown: Allow system to be shut down without having to log on" security option to "Disabled" (only applies to server operating systems)	Disabled
49.03	Failed	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Disabled

Section 50: Security Options (System Cryptography)

The checks in this section verify that the system enforces strong protection for user cryptographic keys stored locally.

1 Benchmark Results

Ref.	Result	Title	Configured Value
50.01	Failed	Set the "System cryptography: Force strong key protection for user keys stored on the computer" security option to "User is prompted when the key is first used" or higher	Not Defined

Section 51: Security Options (System Objects)

The checks in this section verify that the system enforces stricter handling and permissions for internal system objects.

2 Benchmark Results

Ref.	Result	Title	Configured Value
51.01	Passed	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Enabled
51.02	Passed	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" security option to "Enabled"	Enabled

Section 52: Security Options (System Settings)

The checks in this section verify that the system restricts optional subsystem usage and enforces stronger control over how Windows evaluates executable files through Software Restriction Policies.

2 Benchmark Results

Ref.	Result	Title	Configured Value
52.01	Passed	Set the "System settings: Optional subsystems" security option to include only [Empty]	
52.02	Failed	Set the "System settings: Use certificate rules on Windows executables for Software Restriction Policies" security option to "Enabled"	Disabled

Section 53: Security Options (User Account Control)

The checks in this section verify that the system enforces strong User Account Control (UAC) behavior by controlling how elevation prompts are handled, how administrators operate, and how standard users interact with privileged actions.

10 Benchmark Results

Ref.	Result	Title	Configured Value
53.01	Failed	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Not Defined
53.02	Passed	Set the "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" security option to "Disabled"	Disabled
53.03	Failed	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Not Defined
53.04	Failed	Set the "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode" security option to "Prompt for consent on the secure desktop"	Prompt for consent for non-Windows binaries
53.05	Failed	Set the "User Account Control: Behavior of the elevation prompt for standard users" security option to "Automatically deny elevation requests"	Prompt for credentials
53.06	Passed	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Enabled
53.07	Passed	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Enabled
53.08	Passed	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Enabled
53.09	Passed	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Enabled
53.10	Passed	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Enabled

Section 54: Security Options (Windows Connection Manager)

The checks in this section verify that the system controls how network connections are managed, ensuring predictable behavior when devices connect to multiple networks. Minimizing simultaneous connections helps reduce routing ambiguity, prevent traffic from leaking across interfaces, and maintain a clear boundary between domain and non-domain networks.

2 Benchmark Results

Ref.	Result	Title	Configured Value
54.01	Passed	Set the "Windows Connection Manager: Minimize the number of simultaneous connections to the Internet or a Windows Domain" security option to "1 = Minimize simultaneous connections" or "Not Defined"	Not Defined
54.02	Failed	Set the "Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network" security option to "Enabled" on domain members	Not Defined

Section 55: Security Options (Windows Installer)

The checks in this section verify that the system enforces controlled and secure behavior for Windows Installer operations. Restricting user control over installs prevents standard users from manipulating installation processes, while disabling elevated-privilege installs ensures that software cannot silently gain administrative rights.

3 Benchmark Results

Ref.	Result	Title	Configured Value
55.01	Passed	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Not Defined
55.02	Passed	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Not Defined
55.03	Passed	Set the "Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts'" security option to "Disabled" or "Not Defined"	Not Defined

Section 56: Security Options (Windows PowerShell)

The checks in this section verify that the system enables enhanced PowerShell logging features designed to capture detailed script activity and command execution.

2 Benchmark Results

Ref.	Result	Title	Configured Value
56.01	Failed	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Not Defined
56.02	Failed	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Not Defined

Section 57: Security Options (Windows Security)

The checks in this section verify that the system restricts users from modifying key Windows Security settings, particularly those related to app and browser protection.

1 Benchmark Results

Ref.	Result	Title	Configured Value
57.01	Failed	Set the "Windows Security: App and browser protection: Prevent users from modifying settings" security option to "Enabled"	Not Defined

About XIA Configuration

XIA Configuration is an IT infrastructure audit and documentation tool that automates the process of collecting and documenting network configurations.