Compliance Benchmark Results

Report Output

CONTOSO TECHNICAL SERVICES

Date	10/08/2018 16:24:17
Author	DEMO2012R2\sysadmin
Version	1.0.0
Product	XIA Configuration Server [10.2.2.20901]

Disclaimer

This document is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and, or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Compliance Benchmark Results

Provides a summary of the results of the benchmarks that have been run for items in the environment.

Reference	Reference Title	Result	Benchmark Name	Name
1.1	Set "Enforce password history" to remember at least 24 passwords	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
1.2	Set "Maximum password age" to 60 days or less	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
1.3	Set "Minimum password age" to at least 1 day(s)	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
1.4	Set "Minimum password length" to 14 or more characters	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
1.5	Set "Password must meet complexity requirements" to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
1.6	Set "Store passwords using reversible encryption" to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
2.1	Set the "Account lockout duration" to 30 minutes or longer	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
2.2	Set the "Account lockout threshold" to greater than 4 and less than 10	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
2.3	Set the "Reset account lockout after" value to between 15 minutes and 30 minutes	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.1	Enable the Windows Firewall domain profile	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.2	Set the Windows Firewall default inbound action of the domain profile to "Block"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.3	Enable the Windows Firewall public profile	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.4	Set the Windows Firewall default inbound action of the public profile to "Block"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.5	Enable the Windows Firewall private profile	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
3.6	Set the Windows Firewall default inbound action of the private profile to "Block"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
4.1	Rename the local Administrator account to a less easily identifiable account name (does not apply to domain controllers)	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
4.2	Disable the local Guest account (does not apply to domain controllers)	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
5.1	Limit the number of server functions to one per server	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.1	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.2	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.3	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO

6.4	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.5	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.6	Set the "Interactive logon: Do not display last user name" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.7	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.8	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.9	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.10	Set the "Interactive logon: Number of previous logons to cache (in case domain controller is not available)" security option to "0" for servers and "0" for workstations	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.11	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.12	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.13	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.14	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.15	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.16	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.17	Set the "Network security: LDAP client signing requirements" security option to "Require signature"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.18	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.19	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.20	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.23	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.24	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.25	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.26	Set the "Domain member: Disable machine account password changes" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.27	Set the "Domain member: Maximum machine account password age" security option to 30 days	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.28	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.29	Set the "Interactive logon: Prompt user to change password before expiration" security option to a value between 5 and 10 days	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.30	Set the "Interactive logon: Require Domain Controller authentication to unlock workstation" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO

6.31	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation" or greater	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.32	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.33	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.34	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.35	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.36	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.37	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.38	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.39	Set the "Microsoft network server: Server SPN target name validation level" security option to "Accept if provided by client" or "Required from client"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.40	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.41	Set the "Network access: Remotely accessible registry paths" security option to the default value or a null (empty) value	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.42	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.43	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.44	Set the "Network access: Sharing and security model for local accounts" security option to "Classic - Local users authenticate as themselves"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.45	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.46	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.47	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" for domain members	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.48	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.49	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"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.50	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"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.51	Set the "Shutdown: Allow system to be shut down without having to log on" security option to "Disabled" (only applies to server operating systems)	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.52	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.53	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO

	security option to "Enabled"			
6.54	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.55	Set the "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.56	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"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.57	Set the "User Account Control: Behavior of the elevation prompt for standard users" security option to "Automatically deny elevation requests"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.58	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.59	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.60	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.61	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
6.62	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.1	Set "Audit: Audit the access of global system objects" to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.2	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.3	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.4	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.5	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.6	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.7	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.8	Set the "Audit Application Group Management" advanced audit policy to "None"	Warning	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.9	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.10	Set the "Audit Distribution Group Management" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.11	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.12	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.13	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.14	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO

7.16	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.17	Set the "Audit Process Termination" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.18	Set the "Audit RPC Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.23	Set the "Audit Account Lockout" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.25	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.26	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.27	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.28	Set the "Audit Logoff" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.29	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.30	Set the "Audit Network Policy Server" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.31	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.32	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.33	Set the "Audit User/Device Claims" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.34	Set the "Audit Application Generated" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.35	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.36	Set the "Audit Certification Services" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.37	Set the "Audit Detailed File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.38	Set the "Audit File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.39	Set the "Audit File System" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.40	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.41	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.42	Set the "Audit Handle Manipulation" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.43	Set the "Audit Kernel Object" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.44	Set the "Audit Other Object Access Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.45	Set the "Audit Registry" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.46	Set the "Audit Removable Storage" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.47	Set the "Audit SAM" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.48	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO

7.49	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.50	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.51	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.52	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.53	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.54	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.55	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.56	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.57	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.58	Set the "Audit Other System Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.59	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.60	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
7.61	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
8.1	Set the "Sign-in last interactive user automatically after a system-initiated restart" security setting to "Disabled" on Windows Server 2012 R2 and above	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
8.2	Enable Windows Update to receive updates	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
8.3	Configure Windows Update to use Windows Server Update Services (WSUS)	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
9.1	Enable the Windows Time client on all machines	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
9.2	Set the NTP client type to "Domain Hierarchy (NT5DS)" for workstations and member servers, and "NTP" for PDC emulators and machines on workgroups"	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
9.3	Enable the NTP server for domain controllers, and disable for member servers and workstations	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
10.1	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
10.2	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO
11.1	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Failed	Windows Basic Compliance Benchmark	XCS-2K12R2-DEMO