Compliance Benchmark Results

Report Output

CONTOSO FOODS

Date	02 September 2022 17:12:04
Author	TEST2022\sysadmin
Version	1.0.0
Product	XIA Configuration Server [14.1.7.0]

Disclaimer

Compliance Benchmark Results

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

703 Results

Ref.	Item Name	Reference Title	Result	Benchmark Name
1.01	DC-2K22	Set "Enforce password history" to remember at least 24 passwords	Passed	Windows Basic Compliance Benchmark
1.01	XCS-2K22	Set "Enforce password history" to remember at least 24 passwords	Passed	Windows Basic Compliance Benchmark
1.01	XCS-2K22\SQLEXPRESS	Ensure that the SQL instance is running SQL version 11.0 or above	Passed	SQL Basic Compliance Benchmark
1.02	XCS-2K22	Set "Maximum password age" to 60 days or less	Passed	Windows Basic Compliance Benchmark
1.02	DC-2K22	Set "Maximum password age" to 60 days or less	Passed	Windows Basic Compliance Benchmark
1.03	DC-2K22	Set "Minimum password age" to at least 1 day(s)	Passed	Windows Basic Compliance Benchmark
1.03	XCS-2K22	Set "Minimum password age" to at least 1 day(s)	Passed	Windows Basic Compliance Benchmark
1.04	XCS-2K22	Set "Minimum password length" to 14 or more characters	Failed	Windows Basic Compliance Benchmark
1.04	DC-2K22	Set "Minimum password length" to 14 or more characters	Failed	Windows Basic Compliance Benchmark
1.05	DC-2K22	Set "Password must meet complexity requirements" to "Enabled"	Passed	Windows Basic Compliance Benchmark
1.05	XCS-2K22	Set "Password must meet complexity requirements" to "Enabled"	Passed	Windows Basic Compliance Benchmark
1.06	XCS-2K22	Set "Store passwords using reversible encryption" to "Disabled"	Passed	Windows Basic Compliance Benchmark
1.06	DC-2K22	Set "Store passwords using reversible encryption" to "Disabled"	Passed	Windows Basic Compliance Benchmark
2.01	DC-2K22	Set the "Account lockout duration" to 30 minutes or longer	Failed	Windows Basic Compliance Benchmark
2.01	XCS-2K22	Set the "Account lockout duration" to 30 minutes or longer	Failed	Windows Basic Compliance Benchmark
2.01	XCS-2K22\SQLEXPRESS	Disable ad hoc remote queries if not required	Passed	SQL Basic Compliance Benchmark
2.02	XCS-2K22\SQLEXPRESS	Disable CLR integration if not required	Passed	SQL Basic Compliance Benchmark
2.02	XCS-2K22	Set the "Account lockout threshold" to greater than 4 and less than 10	Failed	Windows Basic Compliance Benchmark
2.02	DC-2K22	Set the "Account lockout threshold" to greater than 4 and less than 10	Failed	Windows Basic Compliance Benchmark
2.03	DC-2K22	Set the "Reset account lockout after" value to between 15 minutes and 30 minutes	Failed	Windows Basic Compliance Benchmark

2.03	XCS-2K22	Set the "Reset account lockout after" value to between 15 minutes and 30 minutes	Failed	Windows Basic Compliance Benchmark
2.03	XCS-2K22\SQLEXPRESS	Disable database mail if not required	Passed	SQL Basic Compliance Benchmark
2.04	XCS-2K22\SQLEXPRESS	Disable OLE automation if not required	Passed	SQL Basic Compliance Benchmark
2.05	XCS-2K22\SQLEXPRESS	Disable remote DAC if not required	Passed	SQL Basic Compliance Benchmark
2.06	XCS-2K22\SQLEXPRESS	Disable the service broker endpoint if not required	Passed	SQL Basic Compliance Benchmark
2.07	XCS-2K22\SQLEXPRESS	Disable SOAP endpoints if not required	Passed	SQL Basic Compliance Benchmark
2.08	XCS-2K22\SQLEXPRESS	Disable SQL mail if not required	Passed	SQL Basic Compliance Benchmark
2.09	XCS-2K22\SQLEXPRESS	Disable XP CMD Shell if not required	Passed	SQL Basic Compliance Benchmark
3.01	XCS-2K22\SQLEXPRESS	Rename the 'sa' account	Failed	SQL Basic Compliance Benchmark
3.01	XCS-2K22	Set "Allow Basic Authentication" to "False" for the WinRM Client	Failed	Windows Basic Compliance Benchmark
3.01	DC-2K22	Set "Allow Basic Authentication" to "False" for the WinRM Client	Failed	Windows Basic Compliance Benchmark
3.02	DC-2K22	Set "Allow Digest Authentication" to "False" for the WinRM Client	Failed	Windows Basic Compliance Benchmark
3.02	XCS-2K22	Set "Allow Digest Authentication" to "False" for the WinRM Client	Failed	Windows Basic Compliance Benchmark
3.02	XCS-2K22\SQLEXPRESS	Disable the 'sa' account	Passed	SQL Basic Compliance Benchmark
3.03	XCS-2K22\SQLEXPRESS	Ensure no logins have a blank password	Passed	SQL Basic Compliance Benchmark
3.03	XCS-2K22	Set "Allow Unencrypted Traffic" to "False" for the WinRM Client	Passed	Windows Basic Compliance Benchmark
3.03	DC-2K22	Set "Allow Unencrypted Traffic" to "False" for the WinRM Client	Passed	Windows Basic Compliance Benchmark
3.04	DC-2K22	Set "Allow Basic Authentication" to "False" for the WinRM Service	Passed	Windows Basic Compliance Benchmark
3.04	XCS-2K22	Set "Allow Basic Authentication" to "False" for the WinRM Service	Passed	Windows Basic Compliance Benchmark
3.05	XCS-2K22	Set "Allow Unencrypted Traffic" to "False" for the WinRM Service	Passed	Windows Basic Compliance Benchmark
3.05	DC-2K22	Set "Allow Unencrypted Traffic" to "False" for the WinRM Service	Passed	Windows Basic Compliance Benchmark
3.06	DC-2K22	Set "Disallow Storing RunAs Credentials" to "True" for the WinRM Service	Failed	Windows Basic Compliance Benchmark
3.06	XCS-2K22	Set "Disallow Storing RunAs Credentials" to "True" for the WinRM Service	Failed	Windows Basic Compliance Benchmark
3.07	XCS-2K22	Set "Allow Remote Shell Access" to "True" for the Windows Remote Shell	Passed	Windows Basic Compliance Benchmark
3.07	DC-2K22	Set "Allow Remote Shell Access" to "True" for the Windows Remote Shell	Passed	Windows Basic Compliance Benchmark
4.01	DC-2K22	Rename the local Administrator account to a less easily identifiable account name (does not apply to domain controllers)	Excluded by Platform	Windows Basic Compliance Benchmark
4.01	XCS-2K22	Rename the local Administrator account to a less easily identifiable account name (does not apply to domain controllers)	Failed	Windows Basic Compliance Benchmark

4.01	XCS-2K22\SQLEXPRESS	Set the server authentication mode to 'Windows Authentication Mode'.	Passed	SQL Basic Compliance Benchmark
4.02	XCS-2K22\SQLEXPRESS	Set the server login audit level to 'Failed Logins Only'.	Passed	SQL Basic Compliance Benchmark
4.02	XCS-2K22	Set the local Administrator account to "Disabled" (does not apply to domain controllers)	Failed	Windows Basic Compliance Benchmark
4.02	DC-2K22	Set the local Administrator account to "Disabled" (does not apply to domain controllers)	Excluded by Platform	Windows Basic Compliance Benchmark
4.03	DC-2K22	Rename the local Guest account to a less easily identifiable account name (does not apply to domain controllers)	Excluded by Platform	Windows Basic Compliance Benchmark
4.03	XCS-2K22	Rename the local Guest account to a less easily identifiable account name (does not apply to domain controllers)	Failed	Windows Basic Compliance Benchmark
4.03	XCS-2K22\SQLEXPRESS	Disable cross database ownership chaining	Passed	SQL Basic Compliance Benchmark
4.04	XCS-2K22	Set the local Guest account to "Disabled" (does not apply to domain controllers)	Passed	Windows Basic Compliance Benchmark
4.04	DC-2K22	Set the local Guest account to "Disabled" (does not apply to domain controllers)	Excluded by Platform	Windows Basic Compliance Benchmark
5.01	DC-2K22	Limit the number of server functions to one per server	Failed	Windows Basic Compliance Benchmark
5.01	XCS-2K22	Limit the number of server functions to one per server	Failed	Windows Basic Compliance Benchmark
5.01	XCS-2K22\SQLEXPRESS	Disable scan for start-up procedures	Passed	SQL Basic Compliance Benchmark
6.01	XCS-2K22\SQLEXPRESS	Ensure no databases are configured as TRUSTWORTHY	Passed	SQL Basic Compliance Benchmark
6.01	XCS-2K22	Set "Connection Mode" to "Don't allow remote connections" or "Only allow connections with network level authentication (more secure)"	Passed	Windows Basic Compliance Benchmark
6.01	DC-2K22	Set "Connection Mode" to "Don't allow remote connections" or "Only allow connections with network level authentication (more secure)"	Passed	Windows Basic Compliance Benchmark
6.02	DC-2K22	Set "Disable COM Port Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.02	XCS-2K22	Set "Disable COM Port Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.03	XCS-2K22	Set "Disable Drive Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.03	DC-2K22	Set "Disable Drive Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.04	DC-2K22	Set "Disable LPT Port Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.04	XCS-2K22	Set "Disable LPT Port Redirection" to "True"	Passed	Windows Basic Compliance Benchmark
6.05	XCS-2K22	Set "Disable Plug and Play Device" to "True"	Passed	Windows Basic Compliance Benchmark
6.05	DC-2K22	Set "Disable Plug and Play Device" to "True"	Passed	Windows Basic Compliance Benchmark
6.06	DC-2K22	Set "Always Prompt For Password" to "True"	Passed	Windows Basic Compliance Benchmark
6.06	XCS-2K22	Set "Always Prompt For Password" to "True"	Passed	Windows Basic Compliance Benchmark
6.07	XCS-2K22	Set "Security Layer" to "SSL"	Passed	Windows Basic Compliance Benchmark

6.07	DC-2K22	Set "Security Layer" to "SSL"	Passed	Windows Basic Compliance Benchmark
6.08	DC-2K22	Set "Minimum Encryption Level" to "High"	Passed	Windows Basic Compliance Benchmark
6.08	XCS-2K22	Set "Minimum Encryption Level" to "High"	Passed	Windows Basic Compliance Benchmark
6.09	XCS-2K22	Set "Single Session Restriction" to "True"	Passed	Windows Basic Compliance Benchmark
6.09	DC-2K22	Set "Single Session Restriction" to "True"	Passed	Windows Basic Compliance Benchmark
6.10	DC-2K22	Set "Use Temporary Folders Per Session" to "True"	Passed	Windows Basic Compliance Benchmark
6.10	XCS-2K22	Set "Use Temporary Folders Per Session" to "True"	Passed	Windows Basic Compliance Benchmark
6.11	XCS-2K22	Set "Delete Temporary Folders On Exit" to "True"	Passed	Windows Basic Compliance Benchmark
6.11	DC-2K22	Set "Delete Temporary Folders On Exit" to "True"	Passed	Windows Basic Compliance Benchmark
6.12	DC-2K22	Set "Require Secure RPC Communication" to "True"	Passed	Windows Basic Compliance Benchmark
6.12	XCS-2K22	Set "Require Secure RPC Communication" to "True"	Passed	Windows Basic Compliance Benchmark
7.01	XCS-2K22	Set "Audit: Audit the access of global system objects" to "Disabled"	Passed	Windows Basic Compliance Benchmark
7.01	DC-2K22	Set "Audit: Audit the access of global system objects" to "Disabled"	Passed	Windows Basic Compliance Benchmark
7.01	XCS-2K22\SQLEXPRESS	Disable Named Pipes if not required	Passed	SQL Basic Compliance Benchmark
7.02	DC-2K22	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Passed	Windows Basic Compliance Benchmark
7.02	XCS-2K22	Set "Audit: Audit the use of Backup and Restore privilege" to "Disabled"	Passed	Windows Basic Compliance Benchmark
7.03	XCS-2K22	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Failed	Windows Basic Compliance Benchmark
7.03	DC-2K22	Set "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled"	Failed	Windows Basic Compliance Benchmark
7.04	DC-2K22	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Passed	Windows Basic Compliance Benchmark
7.04	XCS-2K22	Set the "Audit Credential Validation" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.05	XCS-2K22	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.05	DC-2K22	Set the "Audit Kerberos Authentication Service" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.06	DC-2K22	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.06	XCS-2K22	Set the "Audit Kerberos Service Ticket Operations" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.07	XCS-2K22	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark

7.07	DC-2K22	Set the "Audit Other Account Logon Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.08	DC-2K22	Set the "Audit Application Group Management" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.08	XCS-2K22	Set the "Audit Application Group Management" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.09	XCS-2K22	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.09	DC-2K22	Set the "Audit Computer Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.10	DC-2K22	Set the "Audit Distribution Group Management" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.10	XCS-2K22	Set the "Audit Distribution Group Management" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.11	XCS-2K22	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.11	DC-2K22	Set the "Audit Other Account Management Events" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.12	DC-2K22	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.12	XCS-2K22	Set the "Audit Security Group Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.13	XCS-2K22	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.13	DC-2K22	Set the "Audit User Account Management" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.14	DC-2K22	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.14	XCS-2K22	Set the "Audit DPAPI Activity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.15	XCS-2K22	Set the "Audit PNP Activity" advanced audit policy to "Any"	Passed	Windows Basic Compliance Benchmark
7.15	DC-2K22	Set the "Audit PNP Activity" advanced audit policy to "Any"	Passed	Windows Basic Compliance Benchmark
7.16	DC-2K22	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.16	XCS-2K22	Set the "Audit Process Creation" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.17	XCS-2K22	Set the "Audit Process Termination" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.17	DC-2K22	Set the "Audit Process Termination" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.18	DC-2K22	Set the "Audit RPC Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.18	XCS-2K22	Set the "Audit RPC Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.19	XCS-2K22	Set the "Audit Detailed Directory Service Replication" advanced audit policy to "None" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
7.19	DC-2K22	Set the "Audit Detailed Directory Service Replication" advanced audit policy to "None" on domain controllers	Passed	Windows Basic Compliance Benchmark

7.20	DC-2K22	Set the "Audit Directory Service Access" advanced audit policy to "None" on domain controllers	Passed	Windows Basic Compliance Benchmark
7.20	XCS-2K22	Set the "Audit Directory Service Access" advanced audit policy to "None" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
7.21	XCS-2K22	Set the "Audit Directory Service Changes" advanced audit policy to "None" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
7.21	DC-2K22	Set the "Audit Directory Service Changes" advanced audit policy to "None" on domain controllers	Passed	Windows Basic Compliance Benchmark
7.22	DC-2K22	Set the "Audit Directory Service Replication" advanced audit policy to "None" on domain controllers	Passed	Windows Basic Compliance Benchmark
7.22	XCS-2K22	Set the "Audit Directory Service Replication" advanced audit policy to "None" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
7.23	XCS-2K22	Set the "Audit Account Lockout" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.23	DC-2K22	Set the "Audit Account Lockout" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.24	DC-2K22	Set the "Audit Group Membership" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.24	XCS-2K22	Set the "Audit Group Membership" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.25	XCS-2K22	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.25	DC-2K22	Set the "Audit IPsec Extended Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.26	DC-2K22	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.26	XCS-2K22	Set the "Audit IPsec Main Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.27	XCS-2K22	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.27	DC-2K22	Set the "Audit IPsec Quick Mode" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.28	DC-2K22	Set the "Audit Logoff" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.28	XCS-2K22	Set the "Audit Logoff" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.29	XCS-2K22	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.29	DC-2K22	Set the "Audit Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.30	DC-2K22	Set the "Audit Network Policy Server" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.30	XCS-2K22	Set the "Audit Network Policy Server" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.31	XCS-2K22	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.31	DC-2K22	Set the "Audit Other Logon/Logoff Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.32	DC-2K22	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark

7.32	XCS-2K22	Set the "Audit Special Logon" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.33	XCS-2K22	Set the "Audit User/Device Claims" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.33	DC-2K22	Set the "Audit User/Device Claims" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.34	DC-2K22	Set the "Audit Application Generated" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.34	XCS-2K22	Set the "Audit Application Generated" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.35	XCS-2K22	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.35	DC-2K22	Set the "Audit Central Access Policy Staging" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.36	DC-2K22	Set the "Audit Certification Services" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.36	XCS-2K22	Set the "Audit Certification Services" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.37	XCS-2K22	Set the "Audit Detailed File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.37	DC-2K22	Set the "Audit Detailed File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.38	DC-2K22	Set the "Audit File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.38	XCS-2K22	Set the "Audit File Share" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.39	XCS-2K22	Set the "Audit File System" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.39	DC-2K22	Set the "Audit File System" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.40	DC-2K22	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.40	XCS-2K22	Set the "Audit Filtering Platform Connection" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.41	XCS-2K22	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.41	DC-2K22	Set the "Audit Filtering Platform Packet Drop" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.42	DC-2K22	Set the "Audit Handle Manipulation" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.42	XCS-2K22	Set the "Audit Handle Manipulation" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.43	XCS-2K22	Set the "Audit Kernel Object" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.43	DC-2K22	Set the "Audit Kernel Object" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.44	DC-2K22	Set the "Audit Other Object Access Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.44	XCS-2K22	Set the "Audit Other Object Access Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.45	XCS-2K22	Set the "Audit Registry" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.45	DC-2K22	Set the "Audit Registry" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.46	DC-2K22	Set the "Audit Removable Storage" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark

7.46	XCS-2K22	Set the "Audit Removable Storage" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.47	XCS-2K22	Set the "Audit SAM" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.47	DC-2K22	Set the "Audit SAM" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.48	DC-2K22	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.48	XCS-2K22	Set the "Audit Audit Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.49	XCS-2K22	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.49	DC-2K22	Set the "Audit Authentication Policy Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.50	DC-2K22	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.50	XCS-2K22	Set the "Audit Authorization Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.51	XCS-2K22	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.51	DC-2K22	Set the "Audit Filtering Platform Policy Change" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.52	DC-2K22	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.52	XCS-2K22	Set the "Audit MPSSVC Rule-Level Policy Change" advanced audit policy to "Success"	Failed	Windows Basic Compliance Benchmark
7.53	XCS-2K22	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.53	DC-2K22	Set the "Audit Other Policy Change Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.54	DC-2K22	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.54	XCS-2K22	Set the "Audit Non Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.55	XCS-2K22	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.55	DC-2K22	Set the "Audit Other Privilege Use Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.56	DC-2K22	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.56	XCS-2K22	Set the "Audit Sensitive Privilege Use" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.57	XCS-2K22	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.57	DC-2K22	Set the "Audit IPsec Driver" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.58	DC-2K22	Set the "Audit Other System Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.58	XCS-2K22	Set the "Audit Other System Events" advanced audit policy to "None"	Passed	Windows Basic Compliance Benchmark
7.59	XCS-2K22	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.59	DC-2K22	Set the "Audit Security State Change" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.60	DC-2K22	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark

7.60	XCS-2K22	Set the "Audit Security System Extension" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.61	XCS-2K22	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
7.61	DC-2K22	Set the "Audit System Integrity" advanced audit policy to "Success and Failure"	Failed	Windows Basic Compliance Benchmark
8.01	DC-2K22	Enable Windows Update to receive updates	Failed	Windows Basic Compliance Benchmark
8.01	XCS-2K22	Enable Windows Update to receive updates	Failed	Windows Basic Compliance Benchmark
8.02	XCS-2K22	Configure Windows Update to use Windows Server Update Services (WSUS)	Failed	Windows Basic Compliance Benchmark
8.02	DC-2K22	Configure Windows Update to use Windows Server Update Services (WSUS)	Failed	Windows Basic Compliance Benchmark
9.01	DC-2K22	Enable the Windows Time client on all machines	Passed	Windows Basic Compliance Benchmark
9.01	XCS-2K22	Enable the Windows Time client on all machines	Passed	Windows Basic Compliance Benchmark
9.02	XCS-2K22	Set the NTP client type to "Domain Hierarchy (NT5DS)" for domain members and "NTP" for PDC emulators and machines on workgroups	Passed	Windows Basic Compliance Benchmark
9.02	DC-2K22	Set the NTP client type to "Domain Hierarchy (NT5DS)" for domain members and "NTP" for PDC emulators and machines on workgroups	Passed	Windows Basic Compliance Benchmark
9.03	DC-2K22	Enable the NTP server for domain controllers, and disable for all other servers and workstations	Passed	Windows Basic Compliance Benchmark
9.03	XCS-2K22	Enable the NTP server for domain controllers, and disable for all other servers and workstations	Passed	Windows Basic Compliance Benchmark
10.01	XCS-2K22	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark
10.01	DC-2K22	If SNMP is enabled, ensure that no "public" or "private" SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark
10.02	DC-2K22	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark
10.02	XCS-2K22	If SNMP is enabled, ensure that no writable SNMP community strings are configured	Passed	Windows Basic Compliance Benchmark
11.01	XCS-2K22	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Passed	Windows Basic Compliance Benchmark
11.01	DC-2K22	Ensure that Server Message Block (SMB) version 1 is disabled for the server service	Passed	Windows Basic Compliance Benchmark
11.02	DC-2K22	Ensure that Server Message Block (SMB) version 1 is disabled for the client	Passed	Windows Basic Compliance Benchmark
11.02	XCS-2K22	Ensure that Server Message Block (SMB) version 1 is disabled for the client	Passed	Windows Basic Compliance Benchmark
12.01	XCS-2K22	Set the maximum size of the Application event log to 40,960 KB or greater	Failed	Windows Basic Compliance Benchmark
12.01	DC-2K22	Set the maximum size of the Application event log to 40,960 KB or greater	Failed	Windows Basic Compliance Benchmark
12.02	DC-2K22	Set the maximum size of the Security event log to 81,920 KB or greater	Passed	Windows Basic Compliance Benchmark
12.02	XCS-2K22	Set the maximum size of the Security event log to 81,920 KB or greater	Failed	Windows Basic Compliance Benchmark

12.03	XCS-2K22	Set the maximum size of the Setup event log to 20,480 KB or greater	Failed	Windows Basic Compliance Benchmark
12.03	DC-2K22	Set the maximum size of the Setup event log to 20,480 KB or greater	Failed	Windows Basic Compliance Benchmark
12.04	DC-2K22	Set the maximum size of the System event log to 20,480 KB or greater	Passed	Windows Basic Compliance Benchmark
12.04	XCS-2K22	Set the maximum size of the System event log to 20,480 KB or greater	Passed	Windows Basic Compliance Benchmark
12.05	XCS-2K22	Set the retention policy of the Application event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.05	DC-2K22	Set the retention policy of the Application event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.06	DC-2K22	Set the retention policy of the Security event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.06	XCS-2K22	Set the retention policy of the Security event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.07	XCS-2K22	Set the retention policy of the Setup event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.07	DC-2K22	Set the retention policy of the Setup event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.08	DC-2K22	Set the retention policy of the System event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
12.08	XCS-2K22	Set the retention policy of the System event log to 'Overwrite events as needed'	Passed	Windows Basic Compliance Benchmark
13.01	XCS-2K22	Set the "Access Credential Manager as a trusted caller" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.01	DC-2K22	Set the "Access Credential Manager as a trusted caller" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.02	DC-2K22	Set the Access this computer from the network user right to include only [ENTERPRISE_DOMAIN_CONTROLLERS] BUILTIN\Administrators NT AUTHORITY\Authenticated Users	Failed	Windows Basic Compliance Benchmark
13.02	XCS-2K22	Set the Access this computer from the network user right to include only BUILTIN\Administrators NT AUTHORITY\Authenticated Users	Failed	Windows Basic Compliance Benchmark
13.03	XCS-2K22	Set the "Act as part of the operating system" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.03	DC-2K22	Set the "Act as part of the operating system" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.04	DC-2K22	Set the Add workstations to domain user right to include only BUILTIN\Administrators on domain controllers	Failed	Windows Basic Compliance Benchmark
13.04	XCS-2K22	Set the "Add workstations to domain" user right to [Empty] on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
13.05	XCS-2K22	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\	Passed	Windows Basic Compliance Benchmark
13.05	DC-2K22	Set the Adjust memory quotas for a process user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark

		IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\MSSQL% NT SERVICE\		
13.06	DC-2K22	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	Failed	Windows Basic Compliance Benchmark
13.06	XCS-2K22	Set the Allow log on locally user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Users	Passed	Windows Basic Compliance Benchmark
13.07	XCS-2K22	Set the Allow log on through Remote Desktop Services user right to include only BUILTIN\Administrators BUILTIN\Remote Desktop Users	Passed	Windows Basic Compliance Benchmark
13.07	DC-2K22	Set the Allow log on through Remote Desktop Services user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.08	DC-2K22	Set the Back up files and directories user right to include only BUILTIN\Administrators BUILTIN\Backup Operators BUILTIN\Server Operators	Passed	Windows Basic Compliance Benchmark
13.08	XCS-2K22	Set the Back up files and directories user right to include only BUILTIN\Administrators BUILTIN\Backup Operators	Passed	Windows Basic Compliance Benchmark
13.09	XCS-2K22	Set the "Bypass traverse checking" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.09	DC-2K22	Set the "Bypass traverse checking" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.10	DC-2K22	Set the Change the system time user right to include only BUILTIN\Administrators BUILTIN\Server Operators NT AUTHORITY\LOCAL SERVICE	Passed	Windows Basic Compliance Benchmark
13.10	XCS-2K22	Set the Change the system time user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	Passed	Windows Basic Compliance Benchmark
13.11	XCS-2K22	Set the "Change the time zone" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.11	DC-2K22	Set the "Change the time zone" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.12	DC-2K22	Set the Create a pagefile user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.12	XCS-2K22	Set the Create a pagefile user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark

13.13	XCS-2K22	Set the "Create a token object" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.13	DC-2K22	Set the "Create a token object" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.14	DC-2K22	Set the Create global objects user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	Passed	Windows Basic Compliance Benchmark
13.14	XCS-2K22	Set the Create global objects user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	Passed	Windows Basic Compliance Benchmark
13.15	XCS-2K22	Set the "Create permanent shared objects" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.15	DC-2K22	Set the "Create permanent shared objects" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.16	DC-2K22	Set the Create symbolic links user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.16	XCS-2K22	Set the Create symbolic links user right to include only BUILTIN\Administrators NT VIRTUAL MACHINE\Virtual Machines	Passed	Windows Basic Compliance Benchmark
13.17	XCS-2K22	Set the Debug programs user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.17	DC-2K22	Set the Debug programs user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.18	DC-2K22	Set the Deny access to this computer from the network user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.18	XCS-2K22	Set the Deny access to this computer from the network user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.19	XCS-2K22	Set the Deny log on as a batch job user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.19	DC-2K22	Set the Deny log on as a batch job user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.20	DC-2K22	Set the Deny log on as a service user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.20	XCS-2K22	Set the Deny log on as a service user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.21	XCS-2K22	Set the Deny log on locally user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.21	DC-2K22	Set the Deny log on locally user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark

13.22	DC-2K22	Set the Deny log on through Remote Desktop Services user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.22	XCS-2K22	Set the Deny log on through Remote Desktop Services user right to must include BUILTIN\Guests	Failed	Windows Basic Compliance Benchmark
13.23	XCS-2K22	Set the "Enable computer and user accounts to be trusted for delegation" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.23	DC-2K22	Set the Enable computer and user accounts to be trusted for delegation user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.24	DC-2K22	Set the Force shutdown from a remote system user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.24	XCS-2K22	Set the Force shutdown from a remote system user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.25	XCS-2K22	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	Passed	Windows Basic Compliance Benchmark
13.25	DC-2K22	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	Passed	Windows Basic Compliance Benchmark
13.26	DC-2K22	Set the Impersonate a client after authentication user right to include only BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVICE	Passed	Windows Basic Compliance Benchmark
13.26	XCS-2K22	Set the Impersonate a client after authentication user right to include only BUILTIN\Administrators BUILTIN\IIS_IUSRS NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\SERVIC	Passed	Windows Basic Compliance Benchmark
13.27	XCS-2K22	Set the Increase a process working set user right to include only BUILTIN\Device Owners BUILTIN\Users Window Manager\Window Manager Group	Passed	Windows Basic Compliance Benchmark
13.27	DC-2K22	Set the Increase a process working set user right to include only BUILTIN\Device Owners BUILTIN\Users Window Manager\Window Manager Group	Passed	Windows Basic Compliance Benchmark
13.28	DC-2K22	Set the Increase scheduling priority user right to include only	Passed	Windows Basic Compliance Benchmark

		BUILTIN\Administrators Window Manager\Window Manager Group		
13.28	XCS-2K22	Set the Increase scheduling priority user right to include only BUILTIN\Administrators Window Manager\Window Manager Group	Passed	Windows Basic Compliance Benchmark
13.29	XCS-2K22	Set the Load and unload device drivers user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.29	DC-2K22	Set the Load and unload device drivers user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.30	DC-2K22	Set the "Lock pages in memory" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.30	XCS-2K22	Set the "Lock pages in memory" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.31	XCS-2K22	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	Passed	Windows Basic Compliance Benchmark
13.31	DC-2K22	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	Passed	Windows Basic Compliance Benchmark
13.32	DC-2K22	Set the Log on as a service user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	Passed	Windows Basic Compliance Benchmark
13.32	XCS-2K22	Set the Log on as a service user right to include only IIS APPPOOL\% NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	Failed	Windows Basic Compliance Benchmark
13.33	XCS-2K22	Set the Manage auditing and security log user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.33	DC-2K22	Set the Manage auditing and security log user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.34	DC-2K22	Set the "Modify an object label" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.34	XCS-2K22	Set the "Modify an object label" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.35	XCS-2K22	Set the Modify firmware environment values user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.35	DC-2K22	Set the Modify firmware environment values user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.36	DC-2K22	Set the Obtain an impersonation token for another user in the same session user right to include only	Unknown	Windows Basic Compliance Benchmark

		BUILTIN\Administrators		
13.36	XCS-2K22	Set the Obtain an impersonation token for another user in the same session user right to include only BUILTIN\Administrators	Unknown	Windows Basic Compliance Benchmark
13.37	XCS-2K22	Set the Perform volume maintenance tasks user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.37	DC-2K22	Set the Perform volume maintenance tasks user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.38	DC-2K22	Set the Profile single process user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.38	XCS-2K22	Set the Profile single process user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.39	XCS-2K22	Set the Profile system performance user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	Passed	Windows Basic Compliance Benchmark
13.39	DC-2K22	Set the Profile system performance user right to include only BUILTIN\Administrators NT SERVICE\WdiServiceHost	Passed	Windows Basic Compliance Benchmark
13.40	DC-2K22	Set the "Remove computer from docking station" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.40	XCS-2K22	Set the "Remove computer from docking station" user right to [Any Value]	Passed	Windows Basic Compliance Benchmark
13.41	XCS-2K22	Set the Replace a process level token user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	Passed	Windows Basic Compliance Benchmark
13.41	DC-2K22	Set the Replace a process level token user right to include only IIS APPPOOL\% NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\NETWORK SERVICE NT SERVICE\%	Passed	Windows Basic Compliance Benchmark
13.42	DC-2K22	Set the Restore files and directories user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.42	XCS-2K22	Set the Restore files and directories user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.43	XCS-2K22	Set the Shut down the system user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.43	DC-2K22	Set the Shut down the system user right to include only BUILTIN\Administrators	Failed	Windows Basic Compliance Benchmark
13.44	DC-2K22	Set the "Synchronize directory service data" user right to [Empty]	Passed	Windows Basic Compliance Benchmark
13.44	XCS-2K22	Set the "Synchronize directory service data" user right to [Empty]	Passed	Windows Basic Compliance Benchmark

13.45	XCS-2K22	Set the Take ownership of files or other objects user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
13.45	DC-2K22	Set the Take ownership of files or other objects user right to include only BUILTIN\Administrators	Passed	Windows Basic Compliance Benchmark
14.01	DC-2K22	Set the Windows Firewall domain profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
14.01	XCS-2K22	Set the Windows Firewall domain profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
14.02	XCS-2K22	Set the Windows Firewall domain profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
14.02	DC-2K22	Set the Windows Firewall domain profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
14.03	DC-2K22	Set the Windows Firewall domain profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark
14.03	XCS-2K22	Set the Windows Firewall domain profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark
14.04	XCS-2K22	Set the Windows Firewall domain profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
14.04	DC-2K22	Set the Windows Firewall domain profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
14.05	DC-2K22	Set the Windows Firewall domain profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
14.05	XCS-2K22	Set the Windows Firewall domain profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
14.06	XCS-2K22	Set the Windows Firewall domain profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\DomainProfile.log"	Failed	Windows Basic Compliance Benchmark
14.06	DC-2K22	Set the Windows Firewall domain profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\DomainProfile.log"	Failed	Windows Basic Compliance Benchmark
14.07	DC-2K22	Set the Windows Firewall domain profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark
14.07	XCS-2K22	Set the Windows Firewall domain profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark
14.08	XCS-2K22	Set the Windows Firewall domain profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
14.08	DC-2K22	Set the Windows Firewall domain profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
14.09	DC-2K22	Set the Windows Firewall domain profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
14.09	XCS-2K22	Set the Windows Firewall domain profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
15.01	XCS-2K22	Set the Windows Firewall private profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
15.01	DC-2K22	Set the Windows Firewall private profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
15.02	DC-2K22	Set the Windows Firewall private profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
15.02	XCS-2K22	Set the Windows Firewall private profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
15.03	XCS-2K22	Set the Windows Firewall private profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark
15.03	DC-2K22	Set the Windows Firewall private profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark

15.04	DC-2K22	Set the Windows Firewall private profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
15.04	XCS-2K22	Set the Windows Firewall private profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
15.05	XCS-2K22	Set the Windows Firewall private profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
15.05	DC-2K22	Set the Windows Firewall private profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
15.06	DC-2K22	Set the Windows Firewall private profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PrivateProfile.log"	Failed	Windows Basic Compliance Benchmark
15.06	XCS-2K22	Set the Windows Firewall private profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PrivateProfile.log"	Failed	Windows Basic Compliance Benchmark
15.07	XCS-2K22	Set the Windows Firewall private profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark
15.07	DC-2K22	Set the Windows Firewall private profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark
15.08	DC-2K22	Set the Windows Firewall private profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
15.08	XCS-2K22	Set the Windows Firewall private profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
15.09	XCS-2K22	Set the Windows Firewall private profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
15.09	DC-2K22	Set the Windows Firewall private profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
16.01	DC-2K22	Set the Windows Firewall public profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
16.01	XCS-2K22	Set the Windows Firewall public profile firewall state to "On (recommended)"	Passed	Windows Basic Compliance Benchmark
16.02	XCS-2K22	Set the Windows Firewall public profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
16.02	DC-2K22	Set the Windows Firewall public profile default inbound action to "Block (default)"	Passed	Windows Basic Compliance Benchmark
16.03	DC-2K22	Set the Windows Firewall public profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark
16.03	XCS-2K22	Set the Windows Firewall public profile default outbound action to "Allow (default)"	Passed	Windows Basic Compliance Benchmark
16.04	XCS-2K22	Set the Windows Firewall public profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
16.04	DC-2K22	Set the Windows Firewall public profile display a notification setting to "No"	Passed	Windows Basic Compliance Benchmark
16.05	DC-2K22	Set the Windows Firewall public profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
16.05	XCS-2K22	Set the Windows Firewall public profile excluded network interfaces to none	Passed	Windows Basic Compliance Benchmark
16.06	XCS-2K22	Set the Windows Firewall public profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PublicProfile.log"	Failed	Windows Basic Compliance Benchmark
16.06	DC-2K22	Set the Windows Firewall public profile log file path to "%SystemRoot%\System32\LogFiles\Firewall\PublicProfile.log"	Failed	Windows Basic Compliance Benchmark
16.07	DC-2K22	Set the Windows Firewall public profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark
16.07	XCS-2K22	Set the Windows Firewall public profile log file size limit to 16,384 KB or greater	Failed	Windows Basic Compliance Benchmark

16.08	XCS-2K22	Set the Windows Firewall public profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
16.08	DC-2K22	Set the Windows Firewall public profile log dropped packets setting to "Yes"	Failed	Windows Basic Compliance Benchmark
16.09	DC-2K22	Set the Windows Firewall public profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
16.09	XCS-2K22	Set the Windows Firewall public profile log successful connections setting to "Yes"	Failed	Windows Basic Compliance Benchmark
17.01	XCS-2K22	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.01	DC-2K22	Set the "App Runtime: Allow Microsoft accounts to be optional" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.02	DC-2K22	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.02	XCS-2K22	Set the "Biometrics: Configure enhanced anti-spoofing" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.03	XCS-2K22	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.03	DC-2K22	Set the "Cloud Content: Turn off Microsoft consumer experiences" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.04	DC-2K22	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Failed	Windows Basic Compliance Benchmark
17.04	XCS-2K22	Set the "Connect: Require pin for pairing" security option to "First Time" or "Always"	Failed	Windows Basic Compliance Benchmark
17.05	XCS-2K22	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.05	DC-2K22	Set the "OneDrive: Prevent the usage of OneDrive for file storage" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
17.06	DC-2K22	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
17.06	XCS-2K22	Set the "Regional and Language Options: Allow users to enable online speech recognition services" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
17.07	XCS-2K22	Set the "Windows Ink Workspace: Allow Windows Ink Workspace" security option to "Disabled" or "On, but disallow access above lock"	Failed	Windows Basic Compliance Benchmark
17.07	DC-2K22	Set the "Windows Ink Workspace: Allow Windows Ink Workspace" security option to "Disabled" or "On, but disallow access above lock"	Failed	Windows Basic Compliance Benchmark
18.01	DC-2K22	Set the "Accounts: Block Microsoft accounts" security option to "Users can’t add or log on with Microsoft accounts"	Failed	Windows Basic Compliance Benchmark
18.01	XCS-2K22	Set the "Accounts: Block Microsoft accounts" security option to "Users can’t add or log on with Microsoft accounts"	Failed	Windows Basic Compliance Benchmark
18.02	XCS-2K22	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
18.02	DC-2K22	Set the "Accounts: Limit local account use of blank passwords to console logon only" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark

19.01	DC-2K22	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
19.01	XCS-2K22	Set the "Audit Process Creation: Include command line in process creation events" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
19.02	XCS-2K22	Set the "Audit: Shut down system immediately if unable to log security audits" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
19.02	DC-2K22	Set the "Audit: Shut down system immediately if unable to log security audits" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
20.01	DC-2K22	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
20.01	XCS-2K22	Set the "Credential User Interface: Do not display the password reveal button" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
20.02	XCS-2K22	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
20.02	DC-2K22	Set the "Credential User Interface: Enumerate administrator accounts on elevation" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
21.01	DC-2K22	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Failed	Windows Basic Compliance Benchmark
21.01	XCS-2K22	Set the "Credentials Delegation: Encryption Oracle Remediation" security option to "Force Updated Clients"	Failed	Windows Basic Compliance Benchmark
21.02	XCS-2K22	Set the "Credentials Delegation: Remote host allows delegation of non-exportable credentials" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
21.02	DC-2K22	Set the "Credentials Delegation: Remote host allows delegation of non-exportable credentials" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
22.01	DC-2K22	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 bu	Passed	Windows Basic Compliance Benchmark
22.01	XCS-2K22	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 bu	Passed	Windows Basic Compliance Benchmark
22.02	XCS-2K22	Set the "Data Collection and Preview Builds: Allow Telemetry" security option to "0 - Security [Enterprise Only]" or "1 - Basic" on Windows Server 2016, Windows Server 2019, and Windows 10 prior to bu	Excluded by Platform	Windows Basic Compliance Benchmark
22.02	DC-2K22	Set the "Data Collection and Preview Builds: Allow Telemetry" security option to "0 - Security [Enterprise Only]" or "1 - Basic" on Windows Server 2016, Windows Server 2019, and Windows 10 prior to bu	Excluded by Platform	Windows Basic Compliance Benchmark
22.03	DC-2K22	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
22.03	XCS-2K22	Set the "Data Collection and Preview Builds: Do not show feedback notifications" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark

22.04	XCS-2K22	Set the "Data Collection and Preview Builds: Toggle user control over Insider builds" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
22.04	DC-2K22	Set the "Data Collection and Preview Builds: Toggle user control over Insider builds" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
23.01	DC-2K22	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Failed	Windows Basic Compliance Benchmark
23.01	XCS-2K22	Set the "Devices: Allowed to format and eject removable media" security option to "Administrators"	Failed	Windows Basic Compliance Benchmark
23.02	XCS-2K22	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
23.02	DC-2K22	Set the "Devices: Prevent users from installing printer drivers" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
24.01	DC-2K22	Set the "Domain controller: Allow server operators to schedule tasks" security option to "Disabled" on domain controllers	Passed	Windows Basic Compliance Benchmark
24.01	XCS-2K22	Set the "Domain controller: Allow server operators to schedule tasks" security option to "Disabled" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
24.02	XCS-2K22	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
24.02	DC-2K22	Set the "Domain controller: LDAP server signing requirements" security option to "Require signing" on domain controllers	Failed	Windows Basic Compliance Benchmark
24.03	DC-2K22	Set the "Domain controller: Refuse machine account password changes" security option to "Disabled" on domain controllers	Passed	Windows Basic Compliance Benchmark
24.03	XCS-2K22	Set the "Domain controller: Refuse machine account password changes" security option to "Disabled" on domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
25.01	XCS-2K22	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.01	DC-2K22	Set the "Domain member: Digitally encrypt or sign secure channel data (always)" security option to "Enabled" on domain members	Passed	Windows Basic Compliance Benchmark
25.02	DC-2K22	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.02	XCS-2K22	Set the "Domain member: Digitally encrypt secure channel data (when possible)" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.03	XCS-2K22	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.03	DC-2K22	Set the "Domain member: Digitally sign secure channel data (when possible)" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.04	DC-2K22	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.04	XCS-2K22	Set the "Domain member: Disable machine account password changes" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark

25.05	XCS-2K22	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	Failed	Windows Basic Compliance Benchmark
25.05	DC-2K22	Set the "Domain member: Maximum machine account password age" security option to 30 days on domain members	Failed	Windows Basic Compliance Benchmark
25.06	DC-2K22	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
25.06	XCS-2K22	Set the "Domain member: Require strong (Windows 2000 or later) session key" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
26.01	XCS-2K22	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
26.01	DC-2K22	Set the "AutoPlay Policies: Disallow Autoplay for non-volume devices" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
26.02	DC-2K22	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Failed	Windows Basic Compliance Benchmark
26.02	XCS-2K22	Set the "AutoPlay Policies: Set the default behavior for AutoRun" security option to "Do not execute any autorun commands"	Failed	Windows Basic Compliance Benchmark
26.03	XCS-2K22	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Failed	Windows Basic Compliance Benchmark
26.03	DC-2K22	Set the "AutoPlay Policies: Turn off Autoplay" security option to "All drives"	Failed	Windows Basic Compliance Benchmark
26.04	DC-2K22	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Failed	Windows Basic Compliance Benchmark
26.04	XCS-2K22	Set the "File Explorer: Configure Microsoft Defender SmartScreen" security option to "Warn and prevent bypass"	Failed	Windows Basic Compliance Benchmark
26.05	XCS-2K22	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
26.05	DC-2K22	Set the "File Explorer: Enable Microsoft Defender SmartScreen" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
26.06	DC-2K22	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
26.06	XCS-2K22	Set the "File Explorer: Turn off Data Execution Prevention for Explorer" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
26.07	XCS-2K22	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
26.07	DC-2K22	Set the "File Explorer: Turn off heap termination on corruption" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
26.08	DC-2K22	Set the "File Explorer: Turn off shell protocol protected mode" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
26.08	XCS-2K22	Set the "File Explorer: Turn off shell protocol protected mode" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
27.01	XCS-2K22	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on	Failed	Windows Basic Compliance Benchmark

		domain members		
27.01	DC-2K22	Set the "Group Policy: Continue experiences on this device" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
27.02	DC-2K22	Set the "Group Policy: Registry policy processing: Do not apply during periodic background processing" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
27.02	XCS-2K22	Set the "Group Policy: Registry policy processing: Do not apply during periodic background processing" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
27.03	XCS-2K22	Set the "Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
27.03	DC-2K22	Set the "Group Policy: Registry policy processing: Process even if the Group Policy objects have not changed" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
27.04	DC-2K22	Set the "Group Policy: Turn off background refresh of Group Policy" security option to "Disabled" or "Not Defined" on domain members	Passed	Windows Basic Compliance Benchmark
27.04	XCS-2K22	Set the "Group Policy: Turn off background refresh of Group Policy" security option to "Disabled" or "Not Defined" on domain members	Passed	Windows Basic Compliance Benchmark
28.01	XCS-2K22	Set the "Interactive logon: Do not display last user name" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
28.01	DC-2K22	Set the "Interactive logon: Do not display last user name" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
28.02	DC-2K22	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
28.02	XCS-2K22	Set the "Interactive logon: Do not require CTRL+ALT+DEL" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
28.03	XCS-2K22	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Failed	Windows Basic Compliance Benchmark
28.03	DC-2K22	Set the "Interactive logon: Machine account lockout threshold" security option to a value between 6 and 10.	Failed	Windows Basic Compliance Benchmark
28.04	DC-2K22	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Failed	Windows Basic Compliance Benchmark
28.04	XCS-2K22	Set the "Interactive logon: Machine inactivity limit" security option to 900 seconds or less	Failed	Windows Basic Compliance Benchmark
28.05	XCS-2K22	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark
28.05	DC-2K22	Set the "Interactive logon: Message text for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark
28.06	DC-2K22	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark
28.06	XCS-2K22	Set the "Interactive logon: Message title for users attempting to log on" security option to an appropriate value	Failed	Windows Basic Compliance Benchmark
28.07	XCS-2K22	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 on domain members that are not	Failed	Windows Basic Compliance Benchmark

28.07	DC-2K22	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 on domain members that are not	Excluded by Platform	Windows Basic Compliance Benchmark
28.08	DC-2K22	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
28.08	XCS-2K22	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
28.09	XCS-2K22	Set the "Interactive logon: Require Domain Controller authentication to unlock workstation" security option to "Enabled" on domain members that are not domain controllers	Failed	Windows Basic Compliance Benchmark
28.09	DC-2K22	Set the "Interactive logon: Require Domain Controller authentication to unlock workstation" security option to "Enabled" on domain members that are not domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
28.10	DC-2K22	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation", "Force Logoff", or "Disconnect if a Remote Desktop Services session"	Failed	Windows Basic Compliance Benchmark
28.10	XCS-2K22	Set the "Interactive logon: Smart card removal behavior" security option to "Lock Workstation", "Force Logoff", or "Disconnect if a Remote Desktop Services session"	Failed	Windows Basic Compliance Benchmark
29.01	XCS-2K22	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	Passed	Windows Basic Compliance Benchmark
29.01	DC-2K22	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	Passed	Windows Basic Compliance Benchmark
29.02	DC-2K22	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
29.02	XCS-2K22	Set the "Internet Explorer: Prevent downloading of enclosures" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
30.01	XCS-2K22	Set the "Lanman Workstation: Enable insecure guest logons" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
30.01	DC-2K22	Set the "Lanman Workstation: Enable insecure guest logons" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
31.01	DC-2K22	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.01	XCS-2K22	Set the "Logon: Block user from showing account details on sign-in" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.02	XCS-2K22	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.02	DC-2K22	Set the "Logon: Do not display network selection UI" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.03	DC-2K22	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.03	XCS-2K22	Set the "Logon: Do not enumerate connected users on domain-joined computers" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.04	XCS-2K22	Set the "Logon: Enumerate local users on domain-joined computers" security option to "Disabled" on domain members that are not domain controllers	Failed	Windows Basic Compliance Benchmark

31.04	DC-2K22	Set the "Logon: Enumerate local users on domain-joined computers" security option to "Disabled" on domain members that are not domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
31.05	DC-2K22	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.05	XCS-2K22	Set the "Logon: Turn off app notifications on the lock screen" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
31.06	XCS-2K22	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.06	DC-2K22	Set the "Logon: Turn off picture password sign-in" security option to "Enabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.07	DC-2K22	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.07	XCS-2K22	Set the "Logon: Turn on convenience PIN sign-in" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
31.08	XCS-2K22	Set the "Windows Logon Options: Sign-in and lock last interactive user automatically after a restart" security setting to "Disabled"	Passed	Windows Basic Compliance Benchmark
31.08	DC-2K22	Set the "Windows Logon Options: Sign-in and lock last interactive user automatically after a restart" security setting to "Disabled"	Passed	Windows Basic Compliance Benchmark
32.01	DC-2K22	Set the "Microsoft Accounts: Block all consumer Microsoft account user authentication" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
32.01	XCS-2K22	Set the "Microsoft Accounts: Block all consumer Microsoft account user authentication" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
33.01	XCS-2K22	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Failed	Windows Basic Compliance Benchmark
33.01	DC-2K22	Set the "Microsoft Defender Antivirus: Configure detection for potentially unwanted applications" security option to "Block"	Failed	Windows Basic Compliance Benchmark
33.02	DC-2K22	Set the "Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.02	XCS-2K22	Set the "Microsoft Defender Antivirus: Configure local setting override for reporting to Microsoft MAPS" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.03	XCS-2K22	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
33.03	DC-2K22	Set the "Microsoft Defender Antivirus: Configure Watson events" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
33.04	DC-2K22	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.04	XCS-2K22	Set the "Microsoft Defender Antivirus: Join Microsoft MAPS" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.05	XCS-2K22	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Failed	Windows Basic Compliance Benchmark

33.05	DC-2K22	Set the "Microsoft Defender Antivirus: Prevent users and apps from accessing dangerous websites" security option to "Block"	Failed	Windows Basic Compliance Benchmark
33.06	DC-2K22	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
33.06	XCS-2K22	Set the "Microsoft Defender Antivirus: Scan removable drives" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
33.07	XCS-2K22	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.07	DC-2K22	Set the "Microsoft Defender Antivirus: Turn off Microsoft Defender AntiVirus" security option to "Disabled" or "Not Defined"	Failed	Windows Basic Compliance Benchmark
33.08	DC-2K22	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.08	XCS-2K22	Set the "Microsoft Defender Antivirus: Turn on behavior monitoring" security option to "Enabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
33.09	XCS-2K22	Set the "Microsoft Defender Antivirus: Turn on e-mail scanning" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
33.09	DC-2K22	Set the "Microsoft Defender Antivirus: Turn on e-mail scanning" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
34.01	DC-2K22	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
34.01	XCS-2K22	Set the "Microsoft network client: Digitally sign communications (always)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
34.02	XCS-2K22	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
34.02	DC-2K22	Set the "Microsoft network client: Digitally sign communications (if server agrees)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
34.03	DC-2K22	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
34.03	XCS-2K22	Set the "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
35.01	XCS-2K22	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	Passed	Windows Basic Compliance Benchmark
35.01	DC-2K22	Set the "Microsoft network server: Amount of idle time required before suspending session" security option to "15 minutes"	Passed	Windows Basic Compliance Benchmark
35.02	DC-2K22	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
35.02	XCS-2K22	Set the "Microsoft network server: Digitally sign communications (always)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
35.03	XCS-2K22	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
35.03	DC-2K22	Set the "Microsoft network server: Digitally sign communications (if client agrees)" security	Passed	Windows Basic Compliance Benchmark

		option to "Enabled"		
35.04	DC-2K22	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
35.04	XCS-2K22	Set the "Microsoft network server: Disconnect clients when logon hours expire" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
35.05	XCS-2K22	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
35.05	DC-2K22	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
36.01	DC-2K22	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Failed	Windows Basic Compliance Benchmark
36.01	XCS-2K22	Set the "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
36.02	XCS-2K22	Set the "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Failed	Windows Basic Compliance Benchmark
36.02	DC-2K22	Set the "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Failed	Windows Basic Compliance Benchmark
36.03	DC-2K22	Set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Failed	Windows Basic Compliance Benchmark
36.03	XCS-2K22	Set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" security option to "Highest protection, source routing is completely disabled"	Failed	Windows Basic Compliance Benchmark
36.04	XCS-2K22	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
36.04	DC-2K22	Set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
36.05	DC-2K22	Set the "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds" security option to "300000 or 5 minutes (recommended)"	Passed	Windows Basic Compliance Benchmark
36.05	XCS-2K22	Set the "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds" security option to "300000 or 5 minutes (recommended)"	Failed	Windows Basic Compliance Benchmark
36.06	XCS-2K22	Set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
36.06	DC-2K22	Set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
36.07	DC-2K22	Set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark

36.07	XCS-2K22	Set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
36.08	XCS-2K22	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
36.08	DC-2K22	Set the "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)" security option to "Enabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
36.09	DC-2K22	Set the "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)" security option to 5 seconds or less	Passed	Windows Basic Compliance Benchmark
36.09	XCS-2K22	Set the "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)" security option to 5 seconds or less	Failed	Windows Basic Compliance Benchmark
36.10	XCS-2K22	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Failed	Windows Basic Compliance Benchmark
36.10	DC-2K22	Set the "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted" security option to 3	Failed	Windows Basic Compliance Benchmark
36.11	DC-2K22	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Failed	Windows Basic Compliance Benchmark
36.11	XCS-2K22	Set the "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted" security option to 3	Failed	Windows Basic Compliance Benchmark
36.12	XCS-2K22	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	Failed	Windows Basic Compliance Benchmark
36.12	DC-2K22	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	Passed	Windows Basic Compliance Benchmark
37.01	DC-2K22	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
37.01	XCS-2K22	Set the "DNS Client: Turn off multicast name resolution" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
37.02	XCS-2K22	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Failed	Windows Basic Compliance Benchmark
37.02	DC-2K22	Set the "TCP/IP: NetBT NodeType" security option to "P-node (recommended)"	Failed	Windows Basic Compliance Benchmark
38.01	DC-2K22	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Unknown	Windows Basic Compliance Benchmark
38.01	XCS-2K22	Set the "Network access: Allow anonymous SID/Name translation" security option to "Disabled" (must be set with Group Policy)	Unknown	Windows Basic Compliance Benchmark
38.02	XCS-2K22	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
38.02	DC-2K22	Set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
38.03	DC-2K22	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
38.03	XCS-2K22	Set the "Network access: Do not allow anonymous enumeration of SAM accounts" security	Passed	Windows Basic Compliance Benchmark

		option to "Enabled"		
38.04	XCS-2K22	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
38.04	DC-2K22	Set the "Network access: Do not allow storage of passwords and credentials for network authentication" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
38.05	DC-2K22	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
38.05	XCS-2K22	Set the "Network access: Let Everyone permissions apply to anonymous users" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
38.06	XCS-2K22	Set the Network access: Named Pipes that can be accessed anonymously security option to only contain [Empty]	Passed	Windows Basic Compliance Benchmark
38.06	DC-2K22	Set the Network access: Named Pipes that can be accessed anonymously security option to only contain [Empty]	Failed	Windows Basic Compliance Benchmark
38.07	DC-2K22	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 Softwar	Failed	Windows Basic Compliance Benchmark
38.07	XCS-2K22	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 Softwar	Passed	Windows Basic Compliance Benchmark
38.08	XCS-2K22	Set the Network access: Remotely accessible registry paths security option to include only Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\Curr	Passed	Windows Basic Compliance Benchmark
38.08	DC-2K22	Set the Network access: Remotely accessible registry paths security option to include only Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ProductOptions System\Curr	Passed	Windows Basic Compliance Benchmark
38.09	DC-2K22	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
38.09	XCS-2K22	Set the "Network access: Restrict anonymous access to Named Pipes and Shares" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
38.10	XCS-2K22	Set the "Network access: Restrict clients allowed to make remote calls to SAM" security option to "Administrators: Remote Access: Allow" on stand-alone machines and domain members that are not domain	Failed	Windows Basic Compliance Benchmark
38.10	DC-2K22	Set the "Network access: Restrict clients allowed to make remote calls to SAM" security option to "Administrators: Remote Access: Allow" on stand-alone machines and domain members that are not domain	Excluded by Platform	Windows Basic Compliance Benchmark

38.11	DC-2K22	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Failed	Windows Basic Compliance Benchmark
38.11	XCS-2K22	Set the "Network access: Shares that can be accessed anonymously" security option to an empty value	Failed	Windows Basic Compliance Benchmark
38.12	XCS-2K22	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
38.12	DC-2K22	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
39.01	DC-2K22	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
39.01	XCS-2K22	Set the "Network Connections: Prohibit installation and configuration of Network Bridge on your DNS domain network" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
39.02	XCS-2K22	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
39.02	DC-2K22	Set the "Network Connections: Prohibit use of Internet Connection Sharing on your DNS domain network" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
39.03	DC-2K22	Set the "Network Connections: Require domain users to elevate when setting a network's location" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
39.03	XCS-2K22	Set the "Network Connections: Require domain users to elevate when setting a network's location" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
40.01	XCS-2K22	Set the Network Provider: Hardened UNC Paths security option to *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1	Passed	Windows Basic Compliance Benchmark
40.01	DC-2K22	Set the Network Provider: Hardened UNC Paths security option to *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1	Passed	Windows Basic Compliance Benchmark
41.01	DC-2K22	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
41.01	XCS-2K22	Set the "Network security: Allow Local System to use computer identity for NTLM" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
41.02	XCS-2K22	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
41.02	DC-2K22	Set the "Network security: Allow LocalSystem NULL session fallback" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
41.03	DC-2K22	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
41.03	XCS-2K22	Set the "Network security: Allow PKU2U authentication requests to this computer to use online identities" security option to "Disabled" on domain members	Failed	Windows Basic Compliance Benchmark
41.04	XCS-2K22	Set the "Network security: Configure encryption types allowed for Kerberos" security option	Failed	Windows Basic Compliance Benchmark

		to "AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types" on domain members		
41.04	DC-2K22	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	Failed	Windows Basic Compliance Benchmark
41.05	DC-2K22	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
41.05	XCS-2K22	Set the "Network security: Do not store LAN Manager hash value on next password change" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
41.06	XCS-2K22	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Unknown	Windows Basic Compliance Benchmark
41.06	DC-2K22	Set the "Network security: Force logoff when logon hours expire" security option to "Enabled"	Unknown	Windows Basic Compliance Benchmark
41.07	DC-2K22	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Failed	Windows Basic Compliance Benchmark
41.07	XCS-2K22	Set the "Network security: LAN Manager authentication level" security option to "Send NTLMv2 response only. Refuse LM & NTLM"	Failed	Windows Basic Compliance Benchmark
41.08	XCS-2K22	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Failed	Windows Basic Compliance Benchmark
41.08	DC-2K22	Set the "Network security: LDAP client signing requirements" security option to "Require Signing"	Failed	Windows Basic Compliance Benchmark
41.09	DC-2K22	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
41.09	XCS-2K22	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
41.10	XCS-2K22	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
41.10	DC-2K22	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
42.01	DC-2K22	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
42.01	XCS-2K22	Set the "Personalization: Prevent enabling lock screen camera" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
42.02	XCS-2K22	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
42.02	DC-2K22	Set the "Personalization: Prevent enabling lock screen slide show" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark

43.01	DC-2K22	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
43.01	XCS-2K22	Set the "Recovery console: Allow automatic administrative logon" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
43.02	XCS-2K22	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
43.02	DC-2K22	Set the "Recovery Console: Allow floppy copy and access to drives and folders" security option to "Disabled"	Passed	Windows Basic Compliance Benchmark
44.01	DC-2K22	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
44.01	XCS-2K22	Set the "Remote Assistance: Allow Offer Remote Assistance" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
44.02	XCS-2K22	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
44.02	DC-2K22	Set the "Remote Assistance: Allow Solicited Remote Assistance" security option to "Disabled"	Failed	Windows Basic Compliance Benchmark
45.01	DC-2K22	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
45.01	XCS-2K22	Set the "Remote Desktop Connection Client: Do not allow passwords to be saved" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
46.01	XCS-2K22	Set the "Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication" security option to "Enabled" on domain members that are not domain controllers	Passed	Windows Basic Compliance Benchmark
46.01	DC-2K22	Set the "Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication" security option to "Enabled" on domain members that are not domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
46.02	DC-2K22	Set the "Remote Procedure Call: Restrict Unauthenticated RPC clients" security option to "Authenticated" on domain members that are not domain controllers	Excluded by Platform	Windows Basic Compliance Benchmark
46.02	XCS-2K22	Set the "Remote Procedure Call: Restrict Unauthenticated RPC clients" security option to "Authenticated" on domain members that are not domain controllers	Passed	Windows Basic Compliance Benchmark
47.01	XCS-2K22	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Failed	Windows Basic Compliance Benchmark
47.01	DC-2K22	Set the "Search: Allow Cloud Search" security option to "Disable Cloud Search"	Failed	Windows Basic Compliance Benchmark
47.02	DC-2K22	Set the "Search: Allow indexing of encrypted files" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
47.02	XCS-2K22	Set the "Search: Allow indexing of encrypted files" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
48.01	XCS-2K22	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
48.01	DC-2K22	Set the "Security Providers: WDigest Authentication" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
49.01	DC-2K22	Set the "Early Launch Antimalware: Boot-Start Driver Initialization Policy" security option to	Passed	Windows Basic Compliance Benchmark

		"Good, unknown and bad but critical" or "Not Defined"		
49.01	XCS-2K22	Set the "Early Launch Antimalware: Boot-Start Driver Initialization Policy" security option to "Good, unknown and bad but critical" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
49.02	XCS-2K22	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
49.02	DC-2K22	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
49.03	DC-2K22	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
49.03	XCS-2K22	Set the "Shutdown: Clear virtual memory pagefile" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
50.01	XCS-2K22	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	Failed	Windows Basic Compliance Benchmark
50.01	DC-2K22	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	Failed	Windows Basic Compliance Benchmark
51.01	DC-2K22	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
51.01	XCS-2K22	Set the "System objects: Require case insensitivity for non-Windows subsystems" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
51.02	XCS-2K22	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
51.02	DC-2K22	Set the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
52.01	DC-2K22	Set the System settings: Optional subsystems security option to include only [Empty]	Passed	Windows Basic Compliance Benchmark
52.01	XCS-2K22	Set the System settings: Optional subsystems security option to include only [Empty]	Passed	Windows Basic Compliance Benchmark
52.02	XCS-2K22	Set the "System settings: Use certificate rules on Windows executables for Software Restriction Policies" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
52.02	DC-2K22	Set the "System settings: Use certificate rules on Windows executables for Software Restriction Policies" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
53.01	DC-2K22	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
53.01	XCS-2K22	Set the "User Account Control: Admin Approval Mode for the Built-in Administrator account" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
53.02	XCS-2K22	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
53.02	DC-2K22	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

53.03	DC-2K22	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
53.03	XCS-2K22	Set the "User Account Control: Apply UAC restrictions to local accounts on network logons" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
53.04	XCS-2K22	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
53.04	DC-2K22	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
53.05	DC-2K22	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
53.05	XCS-2K22	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
53.06	XCS-2K22	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.06	DC-2K22	Set the "User Account Control: Detect application installations and prompt for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.07	DC-2K22	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.07	XCS-2K22	Set the "User Account Control: Only elevate UIAccess applications that are installed in secure locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.08	XCS-2K22	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.08	DC-2K22	Set the "User Account Control: Run all administrators in Admin Approval Mode" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.09	DC-2K22	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.09	XCS-2K22	Set the "User Account Control: Switch to the secure desktop when prompting for elevation" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.10	XCS-2K22	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
53.10	DC-2K22	Set the "User Account Control: Virtualize file and registry write failures to per-user locations" security option to "Enabled"	Passed	Windows Basic Compliance Benchmark
54.01	DC-2K22	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"	Passed	Windows Basic Compliance Benchmark
54.01	XCS-2K22	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"	Passed	Windows Basic Compliance Benchmark
54.02	XCS-2K22	Set the "Windows Connection Manager: Prohibit connection to non-domain networks when	Passed	Windows Basic Compliance Benchmark

		connected to domain authenticated network" security option to "Enabled" on domain members		
54.02	DC-2K22	Set the "Windows Connection Manager: Prohibit connection to non-domain networks when connected to domain authenticated network" security option to "Enabled" on domain members	Passed	Windows Basic Compliance Benchmark
55.01	DC-2K22	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
55.01	XCS-2K22	Set the "Windows Installer: Allow user control over installs" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
55.02	XCS-2K22	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
55.02	DC-2K22	Set the "Windows Installer: Always install with elevated privileges" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
55.03	DC-2K22	Set the "Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts'" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
55.03	XCS-2K22	Set the "Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts'" security option to "Disabled" or "Not Defined"	Passed	Windows Basic Compliance Benchmark
56.01	XCS-2K22	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
56.01	DC-2K22	Set the "Windows PowerShell: Turn on PowerShell Script Block Logging" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
56.02	DC-2K22	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
56.02	XCS-2K22	Set the "Windows PowerShell: Turn on PowerShell Transcription" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
57.01	XCS-2K22	Set the "Windows Security: App and browser protection: Prevent users from modifying settings" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark
57.01	DC-2K22	Set the "Windows Security: App and browser protection: Prevent users from modifying settings" security option to "Enabled"	Failed	Windows Basic Compliance Benchmark