Kuok (Singapore) Limited

KSL Microsoft Windows Server 2016 Hardening Guide

This document provides prescriptive guidance for establishing a secure configuration posture for all Microsoft Windows Server 2016 operating systems deployed within KSL.

This guide is adapted from the CIS benchmark listed below, incorporating controls that provides adequate security protection without compromising operational stability of the servers. Details about each of the controls listed in the "Controls" tab of this guide, can be found in the CIS benchmark.

CIS Microsoft Windows Server 2016 Benchmark v1.4.0 (Level 1)

Classification	INTERNAL
Document Reference	N.A.
Document Version	1.0
Document Status	FINAL

Authors	
Name	**Title**
Krishna Mohan Singh	Assistant Manager, Infrastructure
Jonathan Ong	General Manager, Cybersecurity

Revision History		
Version	**Date**	**Summary of Changes**
1.0	17-May-23	First Copy

Control N	Control Name	DC Baseline	MS Baseline	Comments
1.1.1	1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'	Exempted	Exempted	As per our defined access control policy for password history
1.1.2	1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	Yes	Yes	
1.1.3	1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'	Yes	Yes	
1.1.4	1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)'	Exempted	Exempted	As per our defined access control policy 8 characters.
1.1.5	1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Yes	Yes	
1.1.6	1.1.6 Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Yes	Yes	
1.2.1	1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)'	Yes	Yes	
1.2.2	1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	Yes	Yes	
1.2.3	1.2.3 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	Yes	Yes	
2.2.1	2.2.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Yes	Exempted	May not be applicable to MS; this will be classified as high risk change
2.2.2	2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only)	Yes	N.A.	
2.2.3	2.2.3 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.2.4	2.2.4 Ensure 'Act as part of the operating system' is set to 'No One'	Yes	Yes	
2.2.5	2.2.5 Ensure 'Add workstations to domain' is set to 'Administrators' (DC only)	Yes	N.A.	
2.2.6	2.2.6 Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Yes	Yes	
2.2.7	2.2.7 Ensure 'Allow log on locally' is set to 'Administrators'	Yes	Yes	
2.2.8	2.2.8 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only)	Yes	N.A.	
2.2.9	2.2.9 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only)	N.A.	Yes	
2.2.10	2.2.10 Ensure 'Back up files and directories' is set to 'Administrators'	Yes	Yes	
2.2.11	2.2.11 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Yes	Yes	
2.2.12	2.2.12 Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'	Yes	Yes	
2.2.13	2.2.13 Ensure 'Create a pagefile' is set to 'Administrators'	Yes	Yes	
2.2.14	2.2.14 Ensure 'Create a token object' is set to 'No One'	Yes	Yes	
2.2.15	2.2.15 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Yes	Yes	
2.2.16	2.2.16 Ensure 'Create permanent shared objects' is set to 'No One'	Yes	Yes	
2.2.17	2.2.17 Ensure 'Create symbolic links' is set to 'Administrators' (DC only)	Yes	N.A.	
2.2.18	2.2.18 Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.2.19	2.2.19 Ensure 'Debug programs' is set to 'Administrators'	Yes	Yes	
2.2.20	2.2.20 Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only)	Yes	N.A.	
2.2.21	2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.2.22	2.2.22 Ensure 'Deny log on as a batch job' to include 'Guests'	Yes	Yes	
2.2.23	2.2.23 Ensure 'Deny log on as a service' to include 'Guests'	Yes	Yes	
2.2.24	2.2.24 Ensure 'Deny log on locally' to include 'Guests'	Yes	Yes	
2.2.25	2.2.25 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only)	Yes	N.A.	
2.2.26	2.2.26 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only)	N.A.	Yes	
2.2.27	2.2.27 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only)	Yes	N.A.	
2.2.28	2.2.28 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only)	N.A.	Yes	
2.2.29	2.2.29 Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Yes	Yes	
2.2.30	2.2.30 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Yes	Yes	
2.2.31	2.2.31 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only)	Yes	N.A.	
2.2.32	2.2.32 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Ro	N.A.	Yes	
2.2.33	2.2.33 Ensure 'Increase scheduling priority' is set to 'Administrators'	Yes	Yes	
2.2.34	2.2.34 Ensure 'Load and unload device drivers' is set to 'Administrators'	Yes	Yes	
2.2.35	2.2.35 Ensure 'Lock pages in memory' is set to 'No One'	Yes	Yes	
2.2.37	2.2.37 Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only)	Yes	N.A.	
2.2.38	2.2.38 Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only)	N.A.	Yes	
2.2.39	2.2.39 Ensure 'Modify an object label' is set to 'No One'	Yes	Yes	
2.2.40	2.2.40 Ensure 'Modify firmware environment values' is set to 'Administrators'	Yes	Yes	
2.2.41	2.2.41 Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Yes	Yes	
2.2.42	2.2.42 Ensure 'Profile single process' is set to 'Administrators'	Yes	Yes	
2.2.43	2.2.43 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Yes	Yes	
2.2.44	2.2.44 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Yes	Yes	
2.2.45	2.2.45 Ensure 'Restore files and directories' is set to 'Administrators'	Yes	Yes	
2.2.46	2.2.46 Ensure 'Shut down the system' is set to 'Administrators'	Yes	Yes	
2.2.47	2.2.47 Ensure 'Synchronize directory service data' is set to 'No One' (DC only)	Yes	N.A.	
2.2.48	2.2.48 Ensure 'Take ownership of files or other objects' is set to 'Administrators'	Yes	Yes	
2.3.1.1	2.3.1.1 Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.3.1.2	2.3.1.2 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.1.3	2.3.1.3 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only)	N.A.	Yes	
2.3.1.4	2.3.1.4 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	Yes	Yes	
2.3.1.5	2.3.1.5 Configure 'Accounts: Rename administrator account'	Yes	Yes	
2.3.1.6	2.3.1.6 Configure 'Accounts: Rename guest account'	Yes	Yes	
2.3.2.1	2.3.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	Yes	Yes	
2.3.2.2	2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	Yes	Yes	
2.3.4.1	2.3.4.1 Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	Yes	Yes	
2.3.4.2	2.3.4.2 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	Yes	Yes	
2.3.5.1	2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)	Exempted	N.A.	This will be classified as high risk change for DC; will require futher testing
2.3.5.2	2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only)	Yes	N.A.	
2.3.5.3	2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only)	Exempted	N.A.	This will be classified as high risk change for DC; will require futher testing
2.3.5.4	2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)	Exempted	N.A.	This will be classified as high risk change for DC; will require futher testing
2.3.5.5	2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)	Exempted	N.A.	This will be classified as high risk change for DC; will require futher testing
2.3.6.1	2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	Yes	Yes	
2.3.6.2	2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	Yes	Yes	
2.3.6.3	2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	Yes	Yes	
2.3.6.4	2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	Yes	Yes	
2.3.6.5	2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	Yes	Yes	
2.3.6.6	2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	Yes	Yes	
2.3.7.1	2.3.7.1 Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	Yes	Yes	
2.3.7.2	2.3.7.2 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	Yes	Yes	
2.3.7.3	2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	Yes	Yes	
2.3.7.4	2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on'	Yes	Yes	
2.3.7.5	2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on'	Yes	Yes	
2.3.7.7	2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	Yes	Yes	
2.3.7.8	2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.3.7.9	2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	Yes	Yes	
2.3.8.1	2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Yes	Yes	
2.3.8.2	2.3.8.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	Yes	Yes	
2.3.8.3	2.3.8.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	Yes	Yes	
2.3.9.1	2.3.9.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	Yes	Yes	
2.3.9.2	2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	Yes	Yes	
2.3.9.3	2.3.9.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Yes	Yes	
2.3.9.4	2.3.9.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	Yes	Yes	
2.3.9.5	2.3.9.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.3.10.1	2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	Yes	Yes	
2.3.10.2	2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)	N.A.	Yes	
2.3.10.3	2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change

2.3.10.5	2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	Yes	Yes	
2.3.10.6	2.3.10.6 Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only)	Yes	N.A.	
2.3.10.7	2.3.10.7 Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only)	N.A.	Yes	
2.3.10.8	2.3.10.8 Configure 'Network access: Remotely accessible registry paths' is configured - Network access: Remotely accessible registry paths	Yes	Yes	
2.3.10.9	2.3.10.9 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured - Network access: Remotely accessible registry paths and sub-p	Yes	Yes	
2.3.10.10	2.3.10.10 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	Yes	Yes	
2.3.10.11	2.3.10.11 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
2.3.10.12	2.3.10.12 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	Yes	Yes	
2.3.10.13	2.3.10.13 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	Yes	Yes	
2.3.11.1	2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.2	2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.3	2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.4	2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.5	2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	Yes	Yes	
2.3.11.7	2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.6	2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	Yes	Yes	
2.3.11.8	2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	Yes	Yes	
2.3.11.9	2.3.11.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.11.10	2.3.11.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Requ	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
2.3.13.1	2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'	Yes	Yes	
2.3.15.1	2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	Yes	Yes	
2.3.15.2	2.3.15.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	Yes	Yes	
2.3.17.1	2.3.17.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	Yes	Yes	
2.3.17.2	2.3.17.2 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure d	Yes	Yes	
2.3.17.3	2.3.17.3 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	Yes	Yes	
2.3.17.4	2.3.17.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	Yes	Yes	
2.3.17.5	2.3.17.5 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	Yes	Yes	
2.3.17.6	2.3.17.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	Yes	Yes	
2.3.17.7	2.3.17.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	Yes	Yes	
2.3.17.8	2.3.17.8 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	Yes	Yes	
5.1	5.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only)	Yes	N.A.	
9.1.1	9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	Yes	Yes	
9.1.2	9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
9.1.3	9.1.3 Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Yes	Yes	
9.1.4	9.1.4 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	Yes	Yes	
9.1.5	9.1.5 Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' - %SYSTEMROOT%\System32\logfiles\	Yes	Yes	
9.1.6	9.1.6 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Yes	Yes	
9.1.7	9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	Yes	Yes	
9.1.8	9.1.8 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	Yes	Yes	
9.2.1	9.2.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	Yes	Yes	
9.2.2	9.2.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
9.2.3	9.2.3 Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Yes	Yes	
9.2.4	9.2.4 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	Yes	Yes	
9.2.5	9.2.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' - %SYSTEMROOT%\System32\logfiles\f	Yes	Yes	
9.2.6	9.2.6 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Yes	Yes	
9.2.7	9.2.7 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	Yes	Yes	
9.2.8	9.2.8 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	Yes	Yes	
9.3.1	9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	Yes	Yes	
9.3.2	9.3.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
9.3.3	9.3.3 Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	Yes	Yes	
9.3.4	9.3.4 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	Yes	Yes	
9.3.5	9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	Yes	Yes	
9.3.6	9.3.6 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	Yes	Yes	
9.3.7	9.3.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' - %SYSTEMROOT%\System32\logfiles\fire	Yes	Yes	
9.3.8	9.3.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Yes	Yes	
9.3.9	9.3.9 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	Yes	Yes	
9.3.10	9.3.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	Yes	Yes	
17.1.1	17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure'	Yes	Yes	
17.1.2	17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only)	Yes	N.A.	
17.1.3	17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only)	Yes	N.A.	
17.2.1	17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure'	Yes	Yes	
17.2.2	17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only)	Yes	N.A.	
17.2.3	17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only)	Yes	N.A.	
17.2.4	17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only)	Yes	N.A.	
17.2.5	17.2.5 Ensure 'Audit Security Group Management' is set to include 'Success'	Yes	Yes	
17.2.6	17.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure'	Yes	Yes	
17.3.1	17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success'	Yes	Yes	
17.3.2	17.3.2 Ensure 'Audit Process Creation' is set to include 'Success'	Yes	Yes	
17.4.1	17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only)	Yes	N.A.	
17.4.2	17.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only)	Yes	N.A.	
17.5.1	17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure'	Yes	Yes	
17.5.2	17.5.2 Ensure 'Audit Group Membership' is set to include 'Success'	Yes	Yes	
17.5.3	17.5.3 Ensure 'Audit Logoff' is set to include 'Success'	Yes	Yes	
17.5.4	17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure'	Yes	Yes	
17.5.5	17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Yes	Yes	
17.5.6	17.5.6 Ensure 'Audit Special Logon' is set to include 'Success'	Yes	Yes	
17.6.1	17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure'	Yes	Yes	
17.6.2	17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure'	Yes	Yes	
17.6.3	17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	Yes	Yes	
17.6.4	17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Yes	Yes	
17.7.1	17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success'	Yes	Yes	
17.7.2	17.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success'	Yes	Yes	
17.7.3	17.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success'	Yes	Yes	
17.7.4	17.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	Yes	Yes	
17.7.5	17.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	Yes	Yes	
17.8.1	17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	Yes	Yes	
17.9.1	17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	Yes	Yes	

17.9.2	17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure'	Yes	Yes	
17.9.3	17.9.3 Ensure 'Audit Security State Change' is set to include 'Success'	Yes	Yes	
17.9.4	17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success'	Yes	Yes	
17.9.5	17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure'	Yes	Yes	
18.1.1.1	18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	Yes	Yes	
18.1.1.2	18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	Yes	Yes	
18.1.2.2	18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	Yes	Yes	
18.2.1	18.2.1 Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	N.A.	N.A.	Not using LAPS
18.2.2	18.2.2 Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	N.A.	N.A.	Not using LAPS
18.2.3	18.2.3 Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	N.A.	N.A.	Not using LAPS
18.2.4	18.2.4 Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	N.A.	N.A.	Not using LAPS
18.2.5	18.2.5 Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)	N.A.	N.A.	Not using LAPS
18.2.6	18.2.6 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)	N.A.	N.A.	Not using LAPS
18.3.1	18.3.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
18.3.2	18.3.2 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.3.3	18.3.3 Ensure 'Configure SMB v1 server' is set to 'Disabled'	Yes	Yes	
18.3.4	18.3.4 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	Yes	Yes	
18.3.5	18.3.5 Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	Yes	Yes	
18.3.6	18.3.6 Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' - Enabled: P-node (recommended)	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.3.7	18.3.7 Ensure 'WDigest Authentication' is set to 'Disabled' - Disabled	Yes	Yes	
18.4.1	18.4.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	Yes	Yes	
18.4.2	18.4.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, sour	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.3	18.4.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source ro	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.4	18.4.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.6	18.4.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.8	18.4.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.9	18.4.9 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer se	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.4.12	18.4.12 Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.4.1	18.5.4.1 Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.4.2	18.5.4.2 Ensure 'Turn off multicast name resolution' is set to 'Enabled' - Enabled	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.8.1	18.5.8.1 Ensure 'Enable insecure guest logons' is set to 'Disabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.11.2	18.5.11.2 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	Yes	Yes	
18.5.11.3	18.5.11.3 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	Yes	Yes	
18.5.11.4	18.5.11.4 Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	Yes	Yes	
18.5.14.1	18.5.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with 'Require Mutual Authentication' and 'Require Integrity' set for all NETLOGON and SYSVOL shares' - N	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.14.1	18.5.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with 'Require Mutual Authentication' and 'Require Integrity' set for all NETLOGON and SYSVOL shares' - S	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.5.21.1	18.5.21.1 Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connectio	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.6.1	18.6.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	Yes	Yes	
18.6.2	18.6.2 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	Yes	Yes	
18.6.3	18.6.3 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	Yes	Yes	
18.8.3.1	18.8.3.1 Ensure 'Include command line in process creation events' is set to 'Enabled' - Disabled	Yes	Yes	
18.8.4.1	18.8.4.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	Yes	Yes	
18.8.4.2	18.8.4.2 Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	Yes	Yes	
18.8.7.2	18.8.7.2 Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'	Yes	Yes	
18.8.14.1	18.8.14.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	Yes	Yes	
18.8.21.2	18.8.21.2 Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Yes	Yes	
18.8.21.3	18.8.21.3 Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	Yes	Yes	
18.8.21.4	18.8.21.4 Ensure 'Continue experiences on this device' is set to 'Disabled'	Yes	Yes	
18.8.21.5	18.8.21.5 Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	Yes	Yes	
18.8.22.1.1	18.8.22.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	Yes	Yes	
18.8.22.1.5	18.8.22.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	Yes	Yes	
18.8.28.1	18.8.28.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.8.28.2	18.8.28.2 Ensure 'Do not display network selection UI' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.8.28.3	18.8.28.3 Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.8.28.4	18.8.28.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
18.8.28.5	18.8.28.5 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	Yes	Yes	
18.8.28.6	18.8.28.6 Ensure 'Turn off picture password sign-in' is set to 'Enabled'	Yes	Yes	
18.8.28.7	18.8.28.7 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	Yes	Yes	
18.8.34.6.3	18.8.34.6.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	Yes	Yes	
18.8.34.6.4	18.8.34.6.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	Yes	Yes	
18.8.36.1	18.8.36.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	Yes	Yes	
18.8.36.2	18.8.36.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	Yes	Yes	

18.8.37.1	18.8.37.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
18.8.40.1	18.8.40.1 Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only)	Yes	N.A.	
18.9.6.1	18.9.6.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Yes	Yes	
18.9.8.1	18.9.8.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Yes	Yes	
18.9.8.2	18.9.8.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	Yes	Yes	
18.9.8.3	18.9.8.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	Yes	Yes	
18.9.10.1.	18.9.10.1.1 Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	Yes	Yes	
18.9.14.1	18.9.14.1 Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	Yes	Yes	
18.9.14.2	18.9.14.2 Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.15.1	18.9.15.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' - Enabled: Always	Yes	Yes	
18.9.16.1	18.9.16.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' - Enabled	N.A.	Exempted	May not be applicable to MS; this will be classified as high risk change
18.9.16.2	18.9.16.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.17.1	18.9.17.1 Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	Yes	Yes	
18.9.17.3	18.9.17.3 Ensure 'Disable OneSettings Downloads' is set to 'Enabled'	Yes	Yes	
18.9.17.4	18.9.17.4 Ensure 'Do not show feedback notifications' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.17.5	18.9.17.5 Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	Yes	Yes	
18.9.17.6	18.9.17.6 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	Yes	Yes	
18.9.17.7	18.9.17.7 Ensure 'Limit Dump Collection' is set to 'Enabled'	Yes	Yes	
18.9.17.8	18.9.17.8 Ensure 'Toggle user control over Insider builds' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.27.1.	18.9.27.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.27.1.	18.9.27.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' - Enabled: 32,768 or greater	Yes	Yes	
18.9.27.2.	18.9.27.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.27.2.	18.9.27.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' - Enabled: 196,608 or greater	Yes	Yes	
18.9.27.3.	18.9.27.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.27.3.	18.9.27.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' - Enabled: 32,768 or greater	Yes	Yes	
18.9.27.4.	18.9.27.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.27.4.	18.9.27.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' - Enabled: 32,768 or greater	Yes	Yes	
18.9.31.2	18.9.31.2 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.31.3	18.9.31.3 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.31.4	18.9.31.4 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.46.1	18.9.46.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.47.4.	18.9.47.4.1 Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.47.5.	18.9.47.5.3.1 Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' - Enabled: Block	Yes	Yes	
18.9.47.9.	18.9.47.9.1 Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.47.9.	18.9.47.9.2 Ensure 'Turn off real-time protection' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.47.9.	18.9.47.9.3 Ensure 'Turn on behavior monitoring' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.47.9.4	18.9.47.9.4 Ensure 'Turn on script scanning' is set to 'Enabled'	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.47.12	18.9.47.12.1 Ensure 'Scan removable drives' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.47.12	18.9.47.12.2 Ensure 'Turn on e-mail scanning' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.47.15	18.9.47.15 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' - Enabled: Block	Yes	Yes	
18.9.47.16	18.9.47.16 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.58.1	18.9.58.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' - Enabled	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.65.2.1	18.9.65.2.2 Ensure 'Do not allow passwords to be saved' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.65.3.1	18.9.65.3.3.2 Ensure 'Do not allow drive redirection' is set to 'Enabled' - Enabled	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.65.3.9	18.9.65.3.9.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.65.3.9	18.9.65.3.9.2 Ensure 'Require secure RPC communication' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.65.3.9	18.9.65.3.9.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' - Enabled: SSL	Yes	Yes	
18.9.65.3.9	18.9.65.3.9.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.65.3.9	18.9.65.3.9.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' - Enabled: High Level	Yes	Yes	
18.9.65.3.1	18.9.65.3.11.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.65.3.1	18.9.65.3.11.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.66.1	18.9.66.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.67.3	18.9.67.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.85.1.1	18.9.85.1.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' - EnableSmartScreen	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.85.1.1	18.9.85.1.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' - ShellSmartScreenLevel	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.89.2	18.9.89.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' - Enabled: On	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.90.1	18.9.90.1 Ensure 'Allow user control over installs' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.90.2	18.9.90.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.91.1	18.9.91.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.100.1	18.9.100.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'	Yes	Yes	
18.9.100.2	18.9.100.2 Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.102.1	18.9.102.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.102.1	18.9.102.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.102.1	18.9.102.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.102.2	18.9.102.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.102.2	18.9.102.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.102.2	18.9.102.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' - Enabled	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.105.2	18.9.105.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled' - Enabled	Exempted	Exempted	May not be applicable to MS; this will be classified as high risk change and will need further testing for DC.
18.9.108.1	18.9.108.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' - Disabled	Yes	Yes	
18.9.108.2	18.9.108.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled' - Enabled	Yes	Yes	
18.9.108.2	18.9.108.2.2 Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' - Every day'	Yes	Yes	
18.9.108.4	18.9.108.4.1 Ensure 'Manage preview builds' is set to 'Disabled'	Yes	Yes	
18.9.108.4	18.9.108.4.2 Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' - DeferFeatureUpdatesPeriodInDays	Yes	Yes	
18.9.108.4	18.9.108.4.2 Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' - DeferFeatureUpdates	Yes	Yes	
18.9.108.4	18.9.108.4.3 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' - DeferQualityUpdates	Yes	Yes	
18.9.108.4	18.9.108.4.3 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' - DeferQualityUpdatesPeriodInDays	Yes	Yes	
19.1.3.1	19.1.3.1 Ensure 'Enable screen saver' is set to 'Enabled'	Yes	Yes	
19.1.3.2	19.1.3.2 Ensure 'Password protect the screen saver' is set to 'Enabled'	Yes	Yes	
19.1.3.3	19.1.3.3 Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	Yes	Yes	
19.5.1.1	19.5.1.1 Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	Yes	Yes	
19.7.4.1	19.7.4.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	Yes	Yes	
19.7.4.2	19.7.4.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	Yes	Yes	
19.7.8.1	19.7.8.1 Ensure 'Configure Windows spotlight on lock screen' is set to Disabled'	Yes	Yes	
19.7.8.2	19.7.8.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	Yes	Yes	
19.7.8.5	19.7.8.5 Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	Yes	Yes	
19.7.28.1	19.7.28.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	Yes	Yes	
19.7.43.1	19.7.43.1 Ensure 'Always install with elevated privileges' is set to 'Disabled'	Yes	Yes	