Configure Automatic Updates	Enabled: - Auto download and notify for install.	Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates	
Minimum Password Length	8 Characters	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length	
Maximum Password Age	60 Days	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age	
Minimum Password Age	1 day		
Password Complexity	Enabled	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements	
Password History	24 passwords remembered	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history	
Store Passwords using Reversible Encryption	Disabled	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption	
Account Lockout Duration	15 minutes	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account	

		Lockout Policy\Account lockout duration	
Account Lockout Threshold	3 attempts	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold	
Reset Account Lockout After	15 minutes	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after	
Enforce user logon restrictions	Enabled	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Enforce user logon restrictions	
Disconnect clients when logon hours expire	Enabled	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire	
Access Credential Manager as a trusted caller'	Set to 'No One'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller	
Set 'Access this computer from the network'	Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS. Level 1 - Member Server. The recommended state	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network	

	for this setting is: Administrators, Authenticated Users.		
Set 'Act as part of the operating system' to 'No One'		Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system	
Set 'Add workstations to domain' to 'Administrators'	Level 1 - Domain Controller	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain	
Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process	
Set 'Allow log on locally' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally	
Configure 'Allow log on through Remote Desktop Services'	Domain controllers: Administrators. Member servers: Administrators, Remote Desktop Users	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services	
Set 'Back up files and directories' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories	
Set 'Change the system time' to 'Administrators, LOCAL SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\User Rights Assignment\Change the system time	
Set 'Change the time zone' to 'Administrators, LOCAL SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone	
Set 'Create a pagefile' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile	
Set 'Create a token object' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object	
Set 'Create global objects' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects	
Set 'Create permanent shared objects' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects	
Set 'Create symbolic links' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links	
Set 'Debug programs' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\User Rights Assignment\Debug programs	
Set 'Deny access to this computer from the network'	Level 1 - Domain Controller. The recommended state for this setting is to include: Guests, Local account. Level 1 - Member Server. The recommended state for this setting is to include: Guests, Local account and member of Administrators group.	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network	
Set 'Deny log on as a batch job' to include 'Guests'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job	
Set 'Deny log on as a service' to include 'Guests'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service	
Set 'Deny log on locally' to include 'Guests'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally	
Set 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services	
Set 'Enable computer and user accounts to be trusted for delegation'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable	

		computer and user accounts to be trusted for delegation	
Set 'Force shutdown from a remote system' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system	
Set 'Generate security audits' to 'LOCAL SERVICE, NETWORK SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits	
Set 'Impersonate a client after authentication' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication	
Set 'Increase scheduling priority' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority	
Set 'Load and unload device drivers' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers	
Set 'Lock pages in memory' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory	
Set 'Manage auditing and security log' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\User Rights Assignment\Manage auditing and security log	
Set 'Modify an object label' to 'No One'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label	
Set 'Modify firmware environment values' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values	
Set 'Perform volume maintenance tasks' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks	
Set 'Profile single process' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process	
Set 'Profile system performance' to 'Administrators, NT SERVICE\WdiServiceHost'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance	
Set 'Replace a process level token' to 'LOCAL SERVICE, NETWORK SERVICE'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token	
Set 'Restore files and directories' to 'Administrators'	Level 1 - Domain Controller	Computer Configuration\Windows	

	Level 1 - Member Server	Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories	
Set 'Shut down the system' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system	
Set 'Synchronize directory service data' to 'No One'	Level 1 - Domain Controller	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Synchronize directory service data	
Set 'Take ownership of files or other objects' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects	
Set 'Accounts: Guest account status' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status	
Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse	
Configure 'Accounts: Rename administrator account'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account	
Configure 'Accounts: Rename guest account'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local	

		Policies\Security Options\Accounts: Rename guest account	
Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\crashonauditfail Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits	
Set 'Devices: Allowed to format and eject removable media' to 'Administrators'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media	
Set 'Devices: Prevent users from installing printer drivers' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers	

Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled'	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks	
Set 'Domain controller: LDAP server signing requirements' to 'Require signing'	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\ldapserverintegrity Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements	
Set 'Domain controller: Refuse machine account password changes' to 'Disabled'	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes	
Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlo	

		gon\Parameters\requiresignorseal Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)	
Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\sealsecurechannel Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)	
Set 'Domain member: Disable machine account password changes' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\disablepasswordchange Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes	
Set 'Domain member: Maximum machine account password age' to 60 , but not 0	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security	

		Options\Domain member: Maximum machine account password age	
Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\requirestrongkey Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key	
Set 'Interactive logon: Do not display last user name' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name	
Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive	

		logon: Do not require CTRL+ALT+DEL	
Set 'Interactive logon: Machine inactivity limit' to 300 second(s), but not 0	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit	
Configure 'Interactive logon: Message text for users attempting to log on'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on “This system is owned and operated by GOC. Use is restricted to GOC. Authorised users must comply with the GOC IT Security Policy. Usage is monitored; unauthorized users will be prosecuted”	
Configure 'Interactive logon: Message title for users attempting to log on'		Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on “Government Online Centre (GOC)”	
Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '3 or fewer logon(s)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscount Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)	
Set 'Interactive logon: Prompt user to change password before expiration' to 'between 7 and 14 days'		Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\passwordexpirywarning Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration	

Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)	
Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)	
Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers	

Set 'Microsoft network server: Amount of idle time required before suspending session' to '5 minute(s)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\autodisconnect Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session	
Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\requiresecuritysignature Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)	
Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\enablesecuritysignature Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)	

Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\enableforcedlogoff Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire	
Set 'Microsoft network server: Server SPN target name validation level' to 'Accept if provided by client'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\SMBServerNameHardeningLevel Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level	
Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (AutoAdminLogon) Enable Automatic	

		Logon (not recommended)	
Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	
Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	
Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security	

		Options\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	
Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires ' to '300 seconds'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires	
Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90% or less'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	
Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation	

Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts	
Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares	
Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users	

Configure 'Network Access: Named Pipes that can be accessed anonymously'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
Set 'Network access: Remotely accessible registry paths'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths	
Set 'Network access: Remotely accessible registry paths and sub-paths'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows	

		NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths	
Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\restrictnullsessaccess Remediation: Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares	
Set 'Network access: Shares that can be accessed anonymously' to 'None'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously	
Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts	
Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\UseMachineId Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM	

Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\allownullsessionfallback Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback	
Set 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\pku2u\AllowOnlineID Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities	
Set 'Network Security: Configure encryption types allowed for Kerberos' to 'RC4\AES128\AES256\Future types'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionTypes Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos	
Set 'Network security: Do not store LAN Manager hash value	Level 1 - Domain Controller	Audit: HKEY_LOCAL_MAC	

on next password change' to 'Enabled'	Level 1 - Member Server	HINE\System\CurrentControlSet\Control\Lsa\NoLMHash Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change	
Set 'Network security: Force logoff when logon hours expire' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	**Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expire**	
Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level	
Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network	

		security: LDAP client signing requirements	
Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	
Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	
Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\securitylevel Remediation: Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\Security Options\Recovery console: Allow automatic administrative logon	
Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\setcommand Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Recovery console: Allow floppy copy and access to all drives and all folders	
Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on	
Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive Remediation: Computer Configuration\Windows Settings\Security Settings\Local	

		Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems	
Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	
Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account	
Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableUIADesktopToggle Remediation: Computer Configuration\Windows Settings\Security	

		Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	
Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	
Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users	
Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation	
Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations	
Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode	
Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop Remediation: Computer Configuration\Windows	

		Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation	
Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization Remediation: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations	
Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Firewall state	
Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DefaultInboundAction	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Inbound connections	
Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DefaultOutboundAction Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Outbound connections	
Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DisableNotifications Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows	

		Firewall: Domain: Display a notification	
Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DisableUnicastResponsesToMulticastBroadcast Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Allow unicast response	
Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalPolicyMerge Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Apply local firewall rules	
Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalIPsecPolicyMerge	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Apply local connection security rules	
Set 'Windows Firewall: Domain: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\LogFilePath Remediation: To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Name	
Set 'Windows Firewall: Domain: Logging: Size limit (KB)' to '16,384 KB or greater '	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFire	

		wall\DomainProfile\Logging\LogFileSize To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater. Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Size limit (KB)	
Set 'Windows Firewall: Domain: Logging: Log dropped packets' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\LogDroppedPackets Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Log dropped packets	
Set 'Windows Firewall: Domain: Logging: Log successful connections' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Log	

		ging\LogSuccessfulConnections Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging\Windows Firewall: Domain: Logging: Log successful connections	
Set 'Windows Firewall: Private: Firewall state' to 'On (recommended)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\EnableFirewall Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Firewall state	
Set 'Windows Firewall: Private: Inbound connections' to 'Block (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DefaultInboundAction Remediation: To establish the recommended configuration via GP, set the following UI path to Block (default).	

		Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Inbound connections	
Set 'Windows Firewall: Private: Outbound connections' to 'Allow (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DefaultOutboundAction Remediation: To establish the recommended configuration via GP, set the following UI path to Allow (default). Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Outbound connections	
Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DisableNotifications Remediation: To establish the recommended	

		configuration via GP, set the following UI path to Yes (default). Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Display a notification	
Set 'Windows Firewall: Private: Allow unicast response' to 'No'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DisableUnicastResponsesToMulticastBroadcast Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Allow unicast response	
Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\AllowLocalPolicyMerge Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows	

		Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Apply local firewall rules	
Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\AllowLocalIPsecPolicyMerge Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Apply local connection security rules	
Set 'Windows Firewall: Private: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogFilePath Remediation: To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log. Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced	

		Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Name	
Set 'Windows Firewall: Private: Logging: Size limit (KB)' to '16,384 KB or greater'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogFileSize Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Size limit (KB)	
Set 'Windows Firewall: Private: Logging: Log dropped packets' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	**Audit:** HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogDroppedPackets Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Log dropped packets	

Set 'Windows Firewall: Private: Logging: Log successful connections' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogSuccessfulConnections Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging\Windows Firewall: Private: Logging: Log successful connections	
Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\EnableFirewall Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Firewall state	
Set 'Windows Firewall: Public: Inbound connections' to 'Block (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DefaultInboundAction	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Inbound connections	
Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DefaultOutboundAction Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Outbound connections	
Set 'Windows Firewall: Public: Display a notification' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DisableNotifications Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows	

		Firewall: Public: Display a notification	
Set 'Windows Firewall: Public: Allow unicast response' to 'No'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DisableUnicastResponsesToMulticastBroadcast Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Allow unicast response	
Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\AllowLocalPolicyMerge Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Apply local firewall rules	
Set 'Windows Firewall: Public: Apply local connection security rules' to 'No'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\AllowLocalIPsecPolicyMerge	

		Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Apply local connection security rules	
Set 'Windows Firewall: Public: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogFilePath Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Name	
Set 'Windows Firewall: Public: Logging: Size limit (KB)' to '16,384 KB or greater'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogFileSize Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public	

		Profile\Logging\Windows Firewall: Public: Logging: Size limit (KB)	
Set 'Windows Firewall: Public: Logging: Log dropped packets' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogDroppedPackets Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Log dropped packets	
Set 'Windows Firewall: Public: Logging: Log successful connections' to 'Yes'	Level 1 - Domain Controller Level 1 - Member Server	Audit: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogSuccessfulConnections Remediation: Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging\Windows Firewall: Public: Logging: Log successful connections	
Set 'Audit Credential Validation' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	To implement the recommended configuration state, set the following Group	

		Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential Validation	
Set 'Audit Computer Account Management' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: Success and Failure. Remediation: Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Computer Account Management	
Set 'Audit Distribution Group Management' to 'Success and Failure'	Level 1 - Domain Controller	The recommended state for this setting is: Success and Failure. Remediation: Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Distribution Group Management	
Set 'Audit Other Account Management Events' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: Success and Failure. Remediation:	

		To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Other Account Management Events	
Set 'Audit Security Group Management' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	The recommended state for this setting is: Success and Failure. Remediation: Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management	
Set 'Audit User Account Management' to 'Success and Failure'	Level 1 - Domain Controller Level 1 - Member Server	Remediation: To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account	

		Management: User Account Management	
Set 'Audit Process Creation' to 'Success'	Level 1 - Domain Controller Level 1 - Member Server	Remediation: To implement the recommended configuration state, set the following Group Policy setting to Success. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: Process Creation	
Set 'Audit Directory Service Access' to 'Success and Failure'	Level 1 - Domain Controller	Remediation: To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service Access	