How to Configure Security Policy Settings.

: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies \Security Options**

Grouping	Security Policy setting
Accounts	Accounts: Administrator account status Accounts: Block Microsoft accounts Accounts: Guest account status Accounts: Limit local account use of blank passwords to console logon only Accounts: Rename administrator account Accounts: Rename guest account
Audit	Audit: Audit the access of global system objects Audit: Audit the use of Backup and Restore privilege Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Audit: Shut down system immediately if unable to log security audits
DCOM	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
Devices	Devices: Allow undock without having to log on Devices: Allowed to format and eject removable media Devices: Prevent users from installing printer drivers Devices: Restrict CD-ROM access to locally logged-on user only Devices: Restrict floppy access to locally logged-on user only
Domain controller	Domain controller: Allow server operators to schedule tasks Domain controller: LDAP server signing requirements

	Domain controller: Refuse machine account password changes
Domain member	Domain member: Digitally encrypt or sign secure channel data (always) Domain member: Digitally encrypt secure channel data (when possible) Domain member: Digitally sign secure channel data (when possible) Domain member: Disable machine account password changes Domain member: Maximum machine account password age Domain member: Require strong (Windows 2000 or later) session key
Interactive logon	Interactive logon: Display user information when the session is locked Interactive logon: Do not display last user name Interactive logon: Do not require CTRL+ALT+DEL Interactive logon: Machine account lockout threshold Interactive logon: Machine inactivity limit Interactive logon: Message text for users attempting to log on Interactive logon: Message title for users attempting to log on Interactive logon: Number of previous logons to cache (in case domain controller is not available) Interactive logon: Prompt user to change password before expiration Interactive logon: Require Domain Controller authentication to unlock workstation Interactive logon: Require smart card Interactive logon: Smart card removal behavior
Microsoft network client	Microsoft network client: Digitally sign communications (always) Microsoft network client: Digitally sign communications (if server agrees) Microsoft network client: Send unencrypted password to third-party SMB servers
Microsoft network server	Microsoft network server: Amount of idle time required before suspending

	session Microsoft network server: Attempt S4U2Self to obtain claim information Microsoft network server: Digitally sign communications (always) Microsoft network server: Digitally sign communications (if client agrees) Microsoft network server: Disconnect clients when logon hours expire Microsoft network server: Server SPN target name validation level
Network access	Network access: Allow anonymous SID-Name translation Network access: Do not allow anonymous enumeration of SAM accounts Network access: Do not allow anonymous enumeration of SAM accounts and shares Network access: Do not allow storage of passwords and credentials for network authentication Network access: Let Everyone permissions apply to anonymous users Network access: Named Pipes that can be accessed anonymously Network access: Remotely accessible registry paths Network access: Remotely accessible registry paths and subpaths Network access: Restrict anonymous access to Named Pipes and Shares Network access: Shares that can be accessed anonymously Network access: Sharing and security model for local accounts
Network security	Network security: Allow Local System to use computer identity for NTLM Network security: Allow LocalSystem NULL session fallback Network Security: Allow PKU2U authentication requests to this computer to use online identities Network security: Configure encryption types allowed for Kerberos Network security: Do not store LAN Manager hash value on next password

	change Network security: Force logoff when logon hours expire Network security: LAN Manager authentication level Network security: LDAP client signing requirements Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication Network security: Restrict NTLM: Add server exceptions in this domain Network Security: Restrict NTLM: Incoming NTLM Traffic Network Security: Restrict NTLM: NTLM authentication in this domain Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers Network Security: Restrict NTLM: Audit Incoming NTLM Traffic Network Security: Restrict NTLM: Audit NTLM authentication in this domain
Recovery console	Recovery console: Allow automatic administrative logon Recovery console: Allow floppy copy and access to all drives and folders
Shutdown	Shutdown: Allow system to be shut down without having to log on Shutdown: Clear virtual memory pagefile
System cryptography	System cryptography: Force strong key protection for user keys stored on the computer System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
System objects	System objects: Require case insensitivity for non-Windows subsystems System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

System settings	System settings: Optional subsystems System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
User Account Control	User Account Control: Admin Approval Mode for the Built-in Administrator account User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode User Account Control: Behavior of the elevation prompt for standard users User Account Control: Detect application installations and prompt for elevation User Account Control: Only elevate executables that are signed and validated User Account Control: Only elevate UIAccess applications that are installed in secure locations User Account Control: Run all administrators in Admin Approval Mode User Account Control: Switch to the secure desktop when prompting for elevation User Account Control: Virtualize file and registry write failures to per-user locations