Local Policy

Administrators can access the computer's Local Policy via:
Click Start and type secpol.msc -> click the secpol application to open it.
Click the Local Policies and double click **Audit Policy, Security Options or User Rig**

Account Policies

Administrators can access the computer's Account Policies via:

Click Start and type secpol.msc -> click secpol to open it.

Double click Account Policies and click **Password Policy or Account Lockout Policy**

Installed Programs

Administrators can access the computer's Installed Programs via:

Click Start -> Control Panel -> Uninstall a Program (link under Programs)

Local Users and Groups

Administrators can access the computer's Local Users and Groups settings

Click Start -> type lusrmgr.msc -> click lusrmgr to open it.

Startup

Administrators can add items to the computer's Startup configuration via:

Click Start and search for msconfig -> Click the Startup tab in the System Configurati

In addition, Users can add items to the Startup folder:
Click Start -> All Programs -> right click Startup and select Open

Shares

Administrators can view the computer's Shares via:

Open Windows Explorer -> Type \\localhost\ -> press Enter

Alternatively, using the command (cmd) window:

Click Start -> type cmd -> click cmd to open the command window -> type net share.

Windows Updates

Administrators can view or modify the computer's settings for Windows U

Click Start -> type update -> click Windows Update

Scheduled Tasks

Administrators can view or modify the computer's Scheduled Tasks via:

Click Start -> type scheduled tasks -> click the Scheduled Tasks application

Firewall

Administrators can view and modify computer's Firewall settings via:

Click Start -> type Firewall -> click the Windows Firewall with Advanced Security ap

Services

An administrator can view and modify the computer's Windows Services v

Click Start -> type Services -> click the Services application

Other

In the Other Tab, Coaches can configure settings for the host file, Remote Desktop anc

Features

An administrator can view and modify the computer's Windows Features v

Click Start -> type Features -> click Turn Windows Features on or off to open it

Settings to check/change

Local Policy - Audit Policy

1. Audit account logon events
2. Audit account management
3. Audit directory service access
4. Audit logon events
5. Audit object access
6. Audit policy change
7. Audit privilege use
8. Audit process tracking
9. Audit system events

Local Policy - Security Options

10. Accounts: Administrator account status
11. Accounts: Block Microsoft Accounts
12. Accounts: Guest account status
13. Accounts: Limit local account use of blank passwords to console logon only
14. Accounts: Rename administrator account
15. Accounts: Rename guest account
16. Audit: Audit the access of global system objects
17. Audit: Audit the use of Backup and Restore privilege
18. Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
19. Audit: Shut down system immediately if unable to log security audits
20. Devices: Allow undock without having to log on
21. Devices: Allowed to format and eject removable media
22. Devices: Prevent users from installing printer drivers
23. Devices: Restrict CD-ROM access to locally logged-on user only
24. Devices: Restrict floppy access to locally logged-on user only
25. Domain controller: Allow server operators to schedule tasks
26. Domain controller: LDAP server signing requirements
27. Domain controller: Refuse machine account password changes
28. Domain member: Digitally encrypt or sign secure channel data (always)
29. Domain member: Digitally encrypt secure channel data (when possible)
30. Domain member: Digitally sign secure channel data (when possible)
31. Domain member: Disable machine account password changes
32. Domain member: Maximum machine account password age
33. Domain member: Require strong (Windows 2000 or later) session key
34. Interactive logon: Display user information when the session is locked
35. Interactive logon: Do not display last user name
36. Interactive logon: Do not require CTRL+ALT+DEL
37. Interactive logon: Machine account lockout threshold
38. Interactive logon: Machine inactivity limit
39. Interactive logon: Message text for users attempting to log on
40. Interactive logon: Message title for users attempting to log on
41. Interactive logon: Number of previous logons to cache (in case domain controller is not available)

42 Interactive logon: Prompt user to change password before expiration
43 Interactive logon: Require Domain Controller authentication to unlock workstation
44 Interactive logon: Require smart card
45 Interactive logon: Smart card removal behavior
46 Microsoft network client: Digitally sign communications (always)
47 Microsoft network client: Digitally sign communications (if server agrees)
48 Microsoft network client: Send unencrypted password to third-party SMB servers
49 Microsoft network server: Amount of idle time required before suspending session
50 Microsoft network server: Attempt S4U2Self to obtain claim information
51 Microsoft network server: Digitally sign communications (always)
52 Microsoft network server: Digitally sign communications (if client agrees)
53 Microsoft network server: Disconnect clients when logon hours expire
54 Microsoft network server: Server SPN target name validation level
55 Network access: Allow anonymous SID/Name translation
56 Network access: Do not allow anonymous enumeration of SAM accounts
57 Network access: Do not allow anonymous enumeration of SAM accounts and shares
58 Network access: Do not allow storage of passwords and credentials for network authentication
59 Network access: Let Everyone permissions apply to anonymous users
60 Network access: Named Pipes that can be accessed anonymously
61 Network access: Remotely accessible registry paths
62 Network access: Remotely accessible registry paths and sub-paths
63 Network access: Restrict anonymous access to Named Pipes and Shares
64 Network access: Shares that can be accessed anonymously
65 Network access: Sharing and security model for local accounts
66 Network security: Allow Local System to use computer identity for NTLM
67 Network security: Allow LocalSystem NULL session fallback
68 Network security: Allow PKU2U authentication requests to this computer to use online identities
69 Network security: Configure encryption types allowed for Kerberos
70 Network security: Do not store LAN Manager hash value on next password change
71 Network security: Force logoff when logon hours expire
72 Network security: LAN Manager authentication level
73 Network security: LDAP client signing requirements
74 Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
75 Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
76 Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
77 Network security: Restrict NTLM: Add server exceptions in this domain
78 Network security: Restrict NTLM: Audit Incoming NTLM Traffic

79 Network security: Restrict NTLM: Audit NTLM authentication in this domain
80 Network security: Restrict NTLM: Incoming NTLM traffic
81 Network security: Restrict NTLM: NTLM authentication in this domain
82 Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
83 Recovery console: Allow automatic administrative logon
84 Recovery console: Allow floppy copy and access to all drives and all folders
85 Shutdown: Allow system to be shut down without having to log on
86 Shutdown: Clear virtual memory pagefile
87 System cryptography: Force strong key protection for user keys stored on the computer
88 System objects: Require case insensitivity for non-Windows subsystems
89 System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
90 System settings: Optional subsystems
91 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
92 User Account Control: Admin Approval Mode for the Built-in Administrator account
93 User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
94 User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
95 User Account Control: Behavior of the elevation prompt for standard users
96 User Account Control: Detect application installations and prompt for elevation
97 User Account Control: Only elevate executables that are signed and validated
98 User Account Control: Only elevate UIAccess applications that are installed in secure locations
99 User Account Control: Run all administrators in Admin Approval Mode
100 User Account Control: Switch to the secure desktop when prompting for elevation
101 User Account Control: Virtualize file and registry write failures to per-user locations

Local Policy - User Rights Assignment

102 Access Credential Manager as a trusted caller

103 Access this computer from the network

104 Act as part of the operating system
105 Add workstations to domain

106 Adjust memory quotas for a process

107 Allow log on locally

108 Allow log on through Remote Desktop Services

109 Back up files and directories

110 Bypass traverse checking

111 Change the system time

112 Change the time zone

113 Create a pagefile
114 Create a token object

115 Create global objects

116 Create permanent shared objects
117 Create symbolic links
118 Debug Programs
119 Deny access to this computer from the network
120 Deny log on as a batch job
121 Deny log on as a service
122 Deny log on locally
123 Deny log on through Remote Desktop Services
124 Enable computer and user accounts to be trust for delegation
125 Force shutdown from a remote system

126 Generate security audits

127 Impersonate a client after authentication

128 Increase a process working set

129 Increase scheduling priority
130 Load and unload device drivers
131 Lock pages in memory

132 Log on as a batch job

133 Log on as a service
134 Manage auditing and security
135 Modify an object label
136 Modify firmware environment values
137 Perform volume maintenance tasks
138 Profile single process
139 Profile system performance

140 Remove computer from docking station

141 Replace a process level token

142 Restore files and directories

143 Shut down the system

144 Synchronize directory service data
145 Take ownership of files or other objects

Account Policies - Account Lockout Policy

146 Account lockout duration
147 Account lockout threshold
148 Reset account lockout counter after

Account Policies - Password Policy

149 Enforce password history
150 Maximum password age
151 Minimum password age
152 Minimum password length
153 Password must meet complexity requirements
154 Store passwords using reversible encryption

Users

155 alphadog

156 Guest
157 JonathanK
158 LeslieG
159 MirandaM
160 MirandaM
161 SrivatsU

Groups

162 Guests
163 Power Users

Scheduled Tasks

164 GatherNetworkInfo
165 SynchronizeTime
166 SynchronizeTimeZone

Firewall Profiles

167 Domain Profile
168 Domain Profile
169 Domain Profile
170 Domain Profile
171 Domain Profile
172 Private Profile
173 Private Profile
174 Private Profile
175 Private Profile
176 Private Profile
177 Public Profile
178 Public Profile
179 Public Profile
180 Public Profile
181 Public Profile

Firewall - Inbound Rules

182 Inbound Rule for Remote Shutdown (RPC-EP-In)

Services

183 DHCP Client
184 IP Helper
185 Windows Search
186 Windows Time

Roles and Features

187 HTTP Logging
188 Logging Tools
189 IIS Management Console
190 FTP Server
191 Telnet Server

Other

192 Hosts file
193 Remote Desktop

ghts Assignment to modify these settings.

y to modify the settings.

via:

on utility.

pdates via:

plication.

ia:

l can specify files to be removed.

ia:

Success, Failure
Success, Failure
Success, Failure
Success, Failure
Success, Failure
Success, Failure
Success, Failure
Success, Failure
Success, Failure

Enabled
Users can't add Microsoft Accounts
Enabled

Enabled

Name change must not contain "admin"
Name change must not contain "guest"
Enabled
Enabled

Enabled

Enabled
Enabled
Administrators
Enabled
Enabled
Enabled
Enabled
Not Defined
Enabled
Enabled
Enabled
Enabled
Enabled
Any value from 0 to 30
Enabled
Do not display user information
Enabled
Enabled
Any value from 0 to 5
Any value from 0 to 10
Score when not empty
Score when not empty

Any value from 0 to 0

Any value from 0 to 3

Enabled

Enabled
Lock Workstation
Enabled
Enabled

Enabled

Any value from 0 to 5

Default
Enabled
Enabled
Enabled
Off
Enabled
Enabled

Enabled

Enabled

Enabled
Score when empty
System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications
System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Mi
Enabled
Score when empty
Classic - local users authenticate as themselves
Enabled
Enabled

Enabled

AES128_HMAC_SHA1,AES256_HMAC_SHA1

Enabled

Enabled
Send LM & NTLM responses
Negotiate signing

Require 128-bit encryption

Require 128-bit encryption

Score when empty

Score when empty
Enable auditing for domain accounts

Enable for domain accounts to domain servers

Allow all
Deny for domain accounts to domain servers

Audit all

Enabled

Enabled

Enabled
Enabled

User is prompted when the key is first used

Enabled

Enabled

Posix

Enabled

Enabled

Enabled

Prompt for credentials on the secure desktop

Prompt for credentials on the secure desktop

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Backup Operators
Users
Administrators
Everyone

Administrators
NETWORK SERVICE

LOCAL SERVICE
Backup Operators
Users
Administrators
Guest

Remote Desktop Users

Administrators
Backup Operators
Administrators
Window Manager Group
Backup Operators
Users
Administrators
NETWORK SERVICE
LOCAL SERVICE
Everyone
Administrators
LOCAL SERVICE
Users
Administrators
LOCAL SERVICE
Administrators

SERVICE
Administrators
NETWORK SERVICE
LOCAL SERVICE

Administrators
Administrators
Guest

Guest

Administrators
NETWORK SERVICE
LOCAL SERVICE
SERVICE
Administrators
NETWORK SERVICE
LOCAL SERVICE

Window Manager Group

Users
Administrators
Administrators

Performance Log Users
Backup Operators
Administrators

Administrators

Administrators
Administrators
Administrators
Administrators

Users

Administrators
NETWORK SERVICE
LOCAL SERVICE
Backup Operators
Administrators
Backup Operators
Users
Administrators

Administrators

Any value from 1 to 5
Any value from 3 to 5
Any value from 1 to 5

Any value from 3 to 5
Any value from 30 to 90
Any value from 0 to 0
Any value from 8 to 12
Enabled
Disabled

User must change password

Account is disabled:False
User must change password
User must change password
User must change password
Account is disabled:True
User must change password

Student
Cyberpatriot

Delete scheduled task GatherNetworkInfo
Delete scheduled task SynchronizeTime
Delete scheduled task SynchronizeTimeZone

Firewall State: On
Inbound connections: Block all connections
Outbound connections: Allow
Display a notification: No
Allow unicast response: No
Firewall State: On
Inbound connections: Block all connections
Outbound connections: Allow
Display a notification: No
Allow unicast response: No
Firewall State: On
Inbound connections: Block all connections
Outbound connections: Allow
Display a notification: No
Allow unicast response: No

Profile:Public,Private,Domain Enabled:True Protocol: TCP Action:Block the connection LocalAddress:Any

Running - Automatic
Stopped - Disabled
Running - Automatic
Running - Automatic

ItemDisabled
ItemEnabled
ItemDisabled
ItemDisabled
ItemDisabled

Hosts file must contain default entries
Don't allow connections to this computer

Software\Microsoft\Windows NT\CurrentVersion
crosoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows

RemoteAddress:Any LocalPort:RPC-EPMap RemotePort:Any

NT\CurrentVersion\Windows System\CurrentC