CIS Microsoft Windows 10 Enterprise (Release 1909) Benchmark

v1.8.1 - 02-05-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1

Overview 43

Intended Audience 43

Consensus Guidance 43

Typographical Conventions 44

Scoring Information 44

Profile Definitions 45

Acknowledgements 47

Recommendations 48

1 Account Policies 48

1.1 Password Policy 48

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored) 48

1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored) 51

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored) . 53

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored) 55

1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored) 58

1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored) 61

1.2 Account Lockout Policy 63

1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored) 63

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored) 65

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored) 67

2 Local Policies 69

2.1 Audit Policy 69

2.2 User Rights Assignment 70

2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Scored) 70

2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users' (Scored) 72

2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Scored) 74

2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Scored) 76

2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users' (Scored) 78

2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (Scored) 80

2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators' (Scored) 82

2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Scored) 84

2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' (Scored) 87

2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators' (Scored) 89

2.2.11 (L1) Ensure 'Create a token object' is set to 'No One' (Scored) 91

2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored) 93

2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One' (Scored) 95

2.2.14 (L1) Configure 'Create symbolic links' (Scored) 97

2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators' (Scored) 99

2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' (Scored) 101

2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Scored) 103

2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests' (Scored) 105

2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests' (Scored) 107

2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Scored) 109

2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (Scored) 111

2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Scored) 113

2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored) 115

2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored) 117

2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Scored) 120

2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Scored) 122

2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One' (Scored) 124

2.2.28 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (Scored) 126

2.2.29 (L2) Configure 'Log on as a service' (Scored) 128

2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Scored) 130

2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One' (Scored)........ 132

2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Scored) 134

2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Scored) 136

2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators' (Scored) 138

2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Scored) 140

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)........ 142

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators' (Scored) 144

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users' (Scored) 146

2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Scored) 148

2.3 Security Options 150

2.3.1 Accounts 150

2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (Scored) 150

2.3.1.2 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Scored) 153

2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (Scored) 155

2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Scored) 157

2.3.1.5 (L1) Configure 'Accounts: Rename administrator account' (Scored) 159

2.3.1.6 (L1) Configure 'Accounts: Rename guest account' (Scored) 161

2.3.2 Audit 163

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Scored) 163

2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Scored) 166

2.3.3 DCOM 168

2.3.4 Devices 169

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' (Scored) 169

2.3.4.2 (L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Scored) 171

2.3.5 Domain controller 172

2.3.6 Domain member 173

2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Scored) 173

2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Scored) 175

2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Scored) 177

2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Scored) 179

2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Scored) 181

2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Scored) 183

2.3.7 Interactive logon 185

2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Scored) 185

2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Scored) 187

2.3.7.3 (BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0' (Scored) 189

2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Scored) 191

2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Scored) 193

2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Scored) 195

2.3.7.7 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (Scored) 197

2.3.7.8 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Scored) 199

2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Scored) 201

2.3.8 Microsoft network client 203

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Scored) 203

2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Scored) 206

2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Scored) 209

2.3.9 Microsoft network server 211

2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Scored) 211

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Scored) 213

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Scored) 216

2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Scored) 219

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (Scored) 221

2.3.10 Network access 224

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Scored) 224

2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Scored) 226

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (Scored) 228

2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Scored) 230

2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Scored) 232

2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None' (Scored) 234

2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths' (Scored) 236

2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' (Scored) 239

2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Scored) 242

2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (Scored) 245

2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Scored) 247

2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Scored) 249

2.3.11 Network security 251

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Scored) 251

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Scored) 253

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Scored) 255

2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Scored) 257

2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Scored) 259

2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Not Scored) 261

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored) 263

2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Scored) 266

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored) 268

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored) 270

2.3.12 Recovery console 272

2.3.13 Shutdown 272

2.3.14 System cryptography 273

2.3.14.1 (L2) Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher (Scored) 273

2.3.15 System objects 275

2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Scored) 275

2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Scored) 277

2.3.16 System settings 279

2.3.17 User Account Control 279

2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Scored) 279

2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Scored) 282

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Scored) 284

2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Scored) 286

2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Scored) 288

2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Scored) 290

2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Scored) 292

2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Scored) 294

3 Event Log 295

4 Restricted Groups 295

5 System Services 296

5.1 (L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Scored) 296

5.2 (L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Scored) 298

5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Scored) 300

5.4 (L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Scored) 302