

CIS Google ChromeOS Benchmark

v1.1.0 - 08-29-2025

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/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	11
Important Usage Information	11
Key Stakeholders	11
Apply the Correct Version of a Benchmark	12
Exceptions	12
Remediation	13
Summary	13
Target Technology Details	14
Recommendation Order	14
Enforced Defaults	14
Viewing the Resulting Policies in ChromeOS	14
Intended Audience	15
Consensus Guidance	16
Typographical Conventions	17
Recommendation Definitions	18
Title	18
Assessment Status	18
Automated	18
Manual	18
Profile	18
Description	18
Rationale Statement	18
Impact Statement	19
Audit Procedure	19
Remediation Procedure	19
Default Value	19
References	19
CIS Critical Security Controls® (CIS Controls®)	19
Additional Information	19
Profile Definitions	20
Acknowledgements	21
Recommendations	22
1 Directory	22
1.1 Users	23

1.1.1 (L1) Ensure more than one Super Admin account exists (Manual)	24
1.1.2 (L1) Ensure no more than 4 Super Admin accounts exist (Manual)	26
1.1.3 (L1) Ensure Super Admin accounts are used only for Super Admin activities (Manual)	28
2 Chrome	30
2.1 Devices	31
2.1.1 (L1) Review Devices Periodically (Manual)	32
2.2 Enrollment tokens	34
2.2.1 (L1) Ensure Any Unused Enrollment Tokens Are Revoked (Automated)	35
2.3 Settings	37
2.3.1 User & Browser	38
2.3.1.1 General	39
2.3.1.1.1 (L1) Ensure 'Maximum user session length' Is Configured (Automated)	40
2.3.1.1.2 (L1) Ensure 'Custom terms of service' Is Configured (Manual)	42
2.3.1.2 Apps and extensions	44
2.3.1.2.1 (L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)	45
2.3.1.2.2 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)	47
2.3.1.3 Site isolation	49
2.3.1.3.1 (L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)	50
2.3.1.4 Security	52
2.3.1.4.1 (L1) Ensure 'Password manager' is Explicitly Configured (Manual)	53
2.3.1.4.2 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	55
2.3.1.4.3 (L1) Ensure 'Online revocation checks' is set to 'Do not perform online OCSP/CRL checks' (Automated)	57
2.3.1.4.4 (L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)	59
2.3.1.4.5 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	61
2.3.1.4.6 (L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater (Automated)	63
2.3.1.4.7 (L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen' (Manual)	65
2.3.1.4.8 (L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	67
2.3.1.4.9 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)	69
2.3.1.4.10 (L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)	71
2.3.1.4.11 (L2) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)	73
2.3.1.4.12 (L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)	75
2.3.1.4.13 (L1) Ensure 'Google online login frequency' Is Set to '1' (Automated)	77
2.3.1.4.14 (L1) Ensure 'Google online unlock frequency' is set to '1' (Automated)	79
2.3.1.4.15 (L1) Ensure 'SAML single sign-on login frequency is set to 'Every day' (Automated)	81
2.3.1.4.16 (L1) Ensure 'SAML single sign-on unlock frequency is set to '1' (Automated)	83
2.3.1.4.17 (L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)	85
2.3.1.4.18 (L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)	87
2.3.1.4.19 (L1) Ensure 'Certificate transparency legacy CA allowlist' is Not Set (Automated)	89
2.3.1.4.20 (L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates' (Automated)	91

2.3.1.4.21 (L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates' (Automated).....	93
2.3.1.4.22 (L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)	95
2.3.1.4.23 (L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)	97
2.3.1.4.24 (L2) Ensure Advanced Protection Program is configured (Manual)	99
2.3.1.4.25 (L1) Ensure 'Override insecure origin restrictions' is Not Set (Automated)	102
2.3.1.4.26 (L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)	104
2.3.1.4.27 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	106
2.3.1.4.28 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	108
2.3.1.4.29 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated) ...	110
2.3.1.4.30 (L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated) ..	112
2.3.1.5 Remote Access	114
2.3.1.5.1 (L2) Ensure 'Remote access clients' Is Configured (Manual)	115
2.3.1.5.2 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	117
2.3.1.5.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)	119
2.3.1.5.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual).....	121
2.3.1.6 Session Settings	123
2.3.1.6.1 (L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)	124
2.3.1.7 Network	126
2.3.1.7.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	127
2.3.1.7.2 (L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Automated)	129
2.3.1.7.3 (L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)	131
2.3.1.7.4 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated).....	133
2.3.1.7.5 (L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated) ..	135
2.3.1.7.6 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	137
2.3.1.7.7 (L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)	140
2.3.1.7.8 (L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)	142
2.3.1.7.9 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated).....	144
2.3.1.7.10 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)	146
2.3.1.7.11 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)	148
2.3.1.7.12 (L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)	150
2.3.1.8 Content	152
2.3.1.8.1 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated).....	153
2.3.1.8.2 (L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)	155
2.3.1.8.3 (L2) Ensure 'Cookies' is set to 'Session Only' (Automated)	157

2.3.1.8.4 (L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)	159
2.3.1.8.5 (L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual)	161
2.3.1.8.6 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)	163
2.3.1.8.7 (L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)	166
2.3.1.8.8 (L1) Ensure 'Auto open downloaded files' Is Not Set (Automated)	168
2.3.1.8.9 (L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)	170
2.3.1.8.10 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	172
2.3.1.8.11 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)	174
2.3.1.8.12 (L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	176
2.3.1.8.13 (L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)	178
2.3.1.8.14 (L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)	180
2.3.1.9 User experience	182
2.3.1.9.1 (L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated)	183
2.3.1.9.2 (L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)	185
2.3.1.9.3 (L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)	187
2.3.1.9.4 (L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)	189
2.3.1.9.5 (L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)	191
2.3.1.9.6 (L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)	193
2.3.1.9.7 (L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)	195
2.3.1.9.8 (L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)	197
2.3.1.9.9 (L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)	199
2.3.1.9.10 (L2) Ensure 'Native Messaging blocked hosts' is set to '*' (Automated)	201
2.3.1.9.11 (L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated)	203
2.3.1.9.12 (L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated)	205
2.3.1.10 Connected devices	207
2.3.1.11 Omnibox Search Provider	208
2.3.1.11.1 (L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)	209
2.3.1.11.2 (L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)	211
2.3.1.12 Hardware	213
2.3.1.12.1 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)	214
2.3.1.12.2 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	216
2.3.1.12.3 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	218

2.3.1.12.4 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	220
2.3.1.12.5 (L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)	222
2.3.1.12.6 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	224
2.3.1.12.7 (L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)	226
2.3.1.13 User verification	228
2.3.1.13.1 (L2) Ensure 'Verified Mode' Is Set to 'Require verified mode boot for Verified Access' (Manual)	229
2.3.1.14 Browser Reporting	231
2.3.1.14.1 (L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting' (Automated)	232
2.3.1.14.2 (L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours (Automated)	234
2.3.1.15 Chrome Safe Browsing	236
2.3.1.15.1 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting' (Automated)	237
2.3.1.15.2 (L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)	240
2.3.1.15.3 (L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)	242
2.3.1.15.4 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	244
2.3.1.15.5 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	246
2.3.1.15.6 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	248
2.3.1.15.7 (L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	250
2.3.1.15.8 (L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs' (Automated)	253
2.3.1.16 Generative AI	255
2.3.1.16.1 Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)	256
2.3.1.16.2 Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	258
2.3.1.16.3 Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	260
2.3.1.16.4 Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	262
2.3.1.16.5 Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	264
2.3.1.16.6 Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)	266
2.3.1.17 Chrome updates	268
2.3.1.17.1 (L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)	269
2.3.1.17.2 (L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)	272
2.3.1.17.3 (L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)	274
2.3.1.18 Chrome variations	276
2.3.1.18.1 (L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)	277

2.3.1.19 Other settings	280
2.3.1.19.1 (L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)	281
2.3.1.19.2 (L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)	283
2.3.2 Device Settings	285
2.3.2.1 Enrollment and access	286
2.3.2.1.1 (L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping' (Automated)	287
2.3.2.1.2 (L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered' (Automated)	289
2.3.2.1.3 (L2) Ensure 'Verified access' Is Set to 'Enable for content protection' (Manual)	291
2.3.2.1.4 Ensure 'Disabled device return instructions' Is Configured (Automated)	293
2.3.2.2 Sign-in settings	295
2.3.2.2.1 (L1) Ensure 'Guest mode' Is Set to 'Disable guest mode' (Automated)	296
2.3.2.2.2 (L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured (Automated)	298
2.3.2.2.3 (L2) Ensure 'Sign-in screen' Is Set to 'Never show user names and photos' (Automated)	300
2.3.2.2.4 (L1) Ensure 'User data' Is Set to 'Do not erase local user data' (Automated)	302
2.3.2.2.5 (L1) Ensure 'Privacy screen on sign-in screen' Is Set to 'Always enable the privacy screen on sign-in screen' (Automated)	304
2.3.2.2.6 (L1) Ensure 'Show numeric keyboard for password' Is Set to 'Default to a standard keyboard for password input' (Automated)	306
2.3.2.3 Device update settings	308
2.3.2.3.1 Auto-update settings	309
2.3.2.3.1.1 (L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates' (Automated)	310
2.3.2.3.1.2 (L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3 (Automated)	312
2.3.2.3.1.3 (L2) Ensure 'Roll back to target version' Is Set to 'Do not roll back OS' (Automated)	314
2.3.2.3.1.4 (L1) Ensure 'Release channel' Is Set to 'Stable channel' (Automated)	316
2.3.2.3.1.5 (L1) Ensure 'Rollout plan' Is Configured (Manual)	318
2.3.2.3.1.6 (L2) Ensure 'Peer to peer' Is Set to 'Do not allow peer to peer auto update downloads' (Automated)	320
2.3.2.3.1.7 (L2) Ensure 'Enforce updates' Is Configured (Manual)	322
2.3.2.3.1.8 Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads' (Automated)	324
2.3.2.3.2 (L1) Ensure 'Variations' Is Set to 'Enable Chrome variations' (Automated)	326
2.3.2.4 User and device reporting	328
2.3.2.4.1 (L1) Ensure 'Metrics reporting' Is Set to 'Never send metrics to Google' (Automated)	329
2.3.2.4.2 (L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload' (Automated)	331
2.3.2.5 Other settings	333
2.3.2.5.1 (L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication' (Automated)	334
2.3.2.5.2 (L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption' (Automated)	336
2.3.2.6 Security	338
2.3.2.6.1 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	339
2.3.3 Managed guest session settings	341
2.3.3.1 General	342
2.3.3.1.1 (L1) Ensure 'Managed guest session' Is Configured (Manual)	343
2.3.3.1.2 (L1) Ensure 'Maximum user session length' Is Configured (Automated)	345

2.3.3.1.3 (L1) Ensure 'Custom terms of service' Is Configured (Automated).....	347
2.3.3.2 Apps and extensions	349
2.3.3.2.1 (L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)	350
2.3.3.2.2 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated).....	352
2.3.3.3 Security	354
2.3.3.3.1 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	355
2.3.3.3.2 (L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)	357
2.3.3.3.3 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	359
2.3.3.3.4 (L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	361
2.3.3.3.5 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated).....	363
2.3.3.3.6 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	365
2.3.3.3.7 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	367
2.3.3.3.8 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)	369
2.3.3.3.9 (L1) Ensure 'Media picker without user gesture' Is Not Set (Automated)	371
2.3.3.4 Remote access	373
2.3.3.4.1 (L1) Ensure 'Remote access clients' Is Configured (Manual)	374
2.3.3.4.2 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	376
2.3.3.4.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated).....	378
2.3.3.4.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual).....	380
2.3.3.5 Session settings	382
2.3.3.5.1 (L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)	383
2.3.3.6 Network	385
2.3.3.6.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	386
2.3.3.6.2 (L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Manual).....	388
2.3.3.6.3 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated).....	390
2.3.3.6.4 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	392
2.3.3.6.5 (L1) Ensure 'SharedArrayBuffer' Is Set to 'Prevent sites that are not cross-origin isolated from using SharedArrayBuffers' (Manual)	395
2.3.3.6.6 (L1) Ensure 'Globally scoped HTTP authentication cache' is set to 'HTTP authentication credentials are scoped to top-level sites' (Automated).....	397
2.3.3.6.7 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated).....	399
2.3.3.6.8 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks' (Automated).....	401
2.3.3.7 Content	403
2.3.3.7.1 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated).....	404
2.3.3.7.2 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated).....	406
2.3.3.7.3 (L1) Ensure 'Auto open downloaded files' Is Not Set (Automated).....	408

2.3.3.7.4 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	410
2.3.3.7.5 (L1) Ensure 'Allow insecure content on these sites' Is Not Set (Automated)	412
2.3.3.7.6 (L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set (Manual)	414
2.3.3.7.7 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)	416
2.3.3.7.8 (L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)	418
2.3.3.8 Power and shutdown	420
2.3.3.8.1 (L1) Ensure 'Idle settings' Is Configured (Automated)	421
2.3.3.9 Hardware	423
2.3.3.9.1 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access' (Automated)	424
2.3.3.9.2 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	426
2.3.3.9.3 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	428
2.3.3.9.4 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	430
2.3.3.9.5 (L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)	432
2.3.3.9.6 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	434
2.3.3.9.7 (L1) Ensure 'USB device detected notification' Is Set to 'Show notifications when USB devices are detected' (Automated)	436
2.3.3.10 Chrome Safe Browsing	438
2.3.3.10.1 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)	439
2.3.3.10.2 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	442
2.3.3.10.3 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	444
2.3.3.10.4 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	446
2.3.3.10.5 (L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	448
2.3.3.11 Data Controls	450
2.3.3.11.1 (L2) Ensure 'Data controls reporting' Is Set to 'Enable reporting of data control events' (Manual)	451
2.4 Apps & extensions	453
2.4.1 (L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)	454
2.4.2 (L1) Ensure 'App and extension install sources' Is Not Set (Automated)	456
2.4.3 (L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)	459
3 Apps	461
3.1 Google Workspace	462
3.1.1 Gmail	463
3.1.1.1 User Settings	464
3.1.1.1.1 (L1) Ensure users cannot delegate access to their mailbox (Manual)	465
3.1.1.2 Safety	467
3.1.1.2.1 Attachments	468
3.1.1.2.1.1 (L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)	469

3.1.1.2.1.2 (L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual).....	471
3.1.1.2.1.3 (L1) Ensure protection against anomalous attachment types in emails is enabled (Manual).....	473
3.1.1.2.2 Links and external images.....	475
3.1.1.2.2.1 (L1) Ensure link identification behind shortened URLs is enabled (Manual)	476
3.1.1.2.2.2 (L1) Ensure scan linked images for malicious content is enabled (Manual).....	478
3.1.1.2.2.3 (L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual).....	480
4 Rules	482
<i>Appendix: Summary Table.....</i>	<i>483</i>
<i>Appendix: CIS Controls v7 IG 1 Mapped Recommendations</i>	<i>502</i>
<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations</i>	<i>505</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations</i>	<i>513</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>522</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>523</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>528</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>537</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>546</i>
<i>Appendix: Change History</i>	<i>547</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for Google ChromeOS devices. This guide was tested against Google ChromeOS v139. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

IMPORTANT NOTE: This Benchmark assumes that Google ChromeOS devices are managed via Google Workspace.

Recommendation Order

This Benchmark has high-level sections based on various security related concerns (Enforced Defaults, Privacy, etc.). It includes specific recommendations from both the Google Chrome and Google Workspace CIS Benchmarks that also apply to Google ChromeOS.

Enforced Defaults

Many of the settings specified in this Benchmark are also the default settings. These are specified for the following reasons:

1. The default (Unset) setting may have the same effect as what is prescribed, but they allow the user to change these settings at any time. Actually configuring the browser setting to the prescribed value will prevent the user from changing it.
2. Many organizations want the ability to scan systems for Benchmark compliance and configuration drift using CIS (CIS-CAT) or CIS-certified third party tools ([CIS Vendor Partners](#)). Having these settings specified in the Benchmark allows for this.

Viewing the Resulting Policies in ChromeOS

These "Policy" settings can be viewed on a managed Google ChromeOS device directly by typing `chrome://policy/` directly into the Google Chrome address box, or through Google Workspace, <https://admin.google.com>.

For more information on Google ChromeOS management, visit <https://chromeos.google/products/device-management/>

Intended Audience

The Google ChromeOS CIS Benchmarks are written for Google ChromeOS managed through Google admin console, not standalone/workgroup systems.

Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (general use)**

Items in this profile intend to:

- be the starting baseline for most organizations;
- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)**

This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability;
- may negatively inhibit the utility or performance of the technology; and
- limit the ability of remote management/access.

Note: Implementation of Level 2 requires that both Level 1 and Level 2 settings are applied.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Jordan Rakoske

Fletcher Oliver

Joe Goerlich , Siemens AG

Patrick Stoeckle , Siemens AG

John Mahlman

Joseph Musso

Loren Hudziak

Daniel Christopher

Kari Byrd

Editor

Edward Byrd , Center for Internet Security, New York

Josh Franklin

Recommendations

1 Directory

The Directory section of the Google Workspace Admin Console.

1.1 Users

User defined in this domain and their permissions.

1.1.1 (L1) *Ensure more than one Super Admin account exists (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Having more than one Super Admin account is needed primarily so that a single point of failure can be avoided. Also, for larger organizations, having multiple Super Admins can be useful for workload balancing purposes.

Rationale:

From a security point of view, having only a single Super Admin Account can be problematic if this user were unavailable for an extended period of time. Also, Super Admin accounts should never be shared amongst multiple users.

Impact:

There should be no user impact, but Administrators should have a normal (low privilege) and an Administrative (high privilege) account.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Go to **Directory** and click on **Users**, this will show a list of all users
3. Click on **+ Add a filter**, select **Admin role**, check the **Super admin** box, and then select **Apply**
4. The list of Users displayed will only be those with the **Super Admin** role
5. Make sure more than one (1) user is listed

Remediation:






Create at least one additional account with a Super Admin role.

NOTE: A new account should be created vs adding this role to an existing account since Administration tasks should be done through separate Admin accounts.

Default Value:

All Google Workspace tenants will have one Super Admin initially.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

1.1.2 (L1) Ensure no more than 4 Super Admin accounts exist (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Having more than one Super Admin account is needed primarily so that a single point of failure can be avoided, but having too many should be avoided.

Rationale:

From a security point of view, having a large number of Super Admin accounts is a bad practice. In general, all users should be assigned the least privileges needed to do their job. This includes Administrators since not everyone that needs to perform certain administrative functions needs to be a Super Admin. Google Workspaces provides many predefined Administration roles and also allows the creation of Custom Roles with very granular permission selection.

Impact:

There should be no user impact, but Administrators should have a normal (low privilege) and an Administrative (high privilege) account.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Go to **Directory** and click on **Users**, this will show a list of all users
3. Click on **+ Add a filter**, select **Admin role**, check the **Super admin** box, and then select **Apply**
4. The list of Users displayed will only be those with the **Super Admin** role
5. Make sure no more than four (4) users are listed






Remediation:

Reduce the number of accounts with a "Super Admin" role.

Default Value:

All Google Workspace tenants will have one Super Admin initially.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

1.1.3 (L1) Ensure Super Admin accounts are used only for Super Admin activities (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Super Admin accounts have access to all features in the Google Admin console and Admin API and can manage every aspect of your organization's account. Super Admins also have full access to all users' calendars and event details.

It is recommended to give each super administrator two accounts: one for their Super Admin account, and a second account for daily activities. Users should only sign in to a Super Admin account to perform Super Admin tasks, such as setting up 2-Step Verification (2SV), managing billing and user licenses, or helping another admin recover their account. Super administrators should use a separate, non-admin account for day-to-day activities.

Super Admins should sign in as needed to do specific tasks and then sign out. Leaving Super Admin accounts signed in can increase exposure to phishing attacks.

Rationale:

Use the Super Admin account only when needed. Delegate administrator tasks to user accounts with limited admin roles. Use the least privilege approach, where each user has access to only the resources and tools needed for their typical tasks. For example, you could grant an admin permissions to create user accounts and reset passwords, but not let them delete user accounts.

Impact:

Super Admin users will have to switch accounts as well as utilize login/logout functionality when performing administrative tasks.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Go to **Directory** and click on **Users**, this will show a list of all users
3. Click on **+ Add a filter**, select **Admin role**, check the **Super Admin** box, and then select **Apply**
4. The list of Users displayed will only be those with the **Super Admin** role
5. Click on **+ Add a filter**, select **Admin role**, check the **Delegated admin** box, and then select **Apply**
6. Verify that there are no users in both the **Super Admin** and **Delegated admin** roles

Remediation:

For every **Super Admin** that is also a **Delegated admin** account, either create a **Delegated admin** account for the user or elevate their existing non-admin account to a **Delegated admin** account.






Default Value:

N/A

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide>
2. <https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide>
3. <https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#9-use-cloud-native-accounts-for-azure-ad-roles>
4. <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

2 Chrome

The Chrome configuration panel is used to manage ChromeOS and ChromeOS devices.

2.1 Devices

The **Devices** section in Google Workspace allows you to verify your enrolled ChromeOS devices as well as enroll new ChromeOS devices. Administrators should regularly audit the **Devices** and make sure they are part of your organization's fleet of ChromeOS devices.

2.1.1 (L1) Review Devices Periodically (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

All ChromeOS devices that are managed by your organization are listed in the **Devices** section of Google Workspace. It is a best practice to periodically audit the list for any unknown devices as well as remove any devices that are no longer in service.

If any unknown devices are found, they should be investigated.

Rationale:

Performing a periodic review of connected devices ensures only permitted and required devices can access organizational data or resources.

Impact:

This should have no impact on the user or admin.

Audit:

To verify this setting via the Google Workspace Admin Console:







1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Devices**
5. Ensure all listed devices have been properly vetted and authorized by the appropriate personnel

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Devices**
5. Ensure all listed devices have been properly vetted and authorized by the appropriate personnel
6. Now remove any unknown devices

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 <u>Address Unauthorized Assets</u> Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.			
v7	1.6 <u>Address Unauthorized Assets</u> Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.			

2.2 Enrollment tokens

The section of Google Workspace where enrollment tokens for ChromeOS are created and stored.

2.2.1 (L1) Ensure Any Unused Enrollment Tokens Are Revoked (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

An organization should not have any unused enrollment tokens.

Rationale:

Revoking unused enrollment tokens keeps them from being used on unknown devices.

Impact:

There should be no impact on the user of admin.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Enrollment tokens**
5. Ensure all listed enrollment tokens are in use

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Enrollment tokens**
5. Remove any unused enrollment tokens

References:

1. <https://support.google.com/chrome/a/answer/1360534?sjid=17213857381939141708-NC>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3 Settings

The setting section contains both configurations for the **User & browser** section, **Devices** section, and **Managed guest session settings** section.

2.3.1 User & Browser

The **User & browser** section is where Chrome and ChromeOS shared configurations exist.

2.3.1.1 General

2.3.1.1.1 (L1) Ensure 'Maximum user session length' Is Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This control sets the length of time that a session can run before the user is logged out and the session is terminated. The user is shown in the system tray how much time is remaining before they will be automatically logged out.

The values are between 1 minute to 1440 minutes. If no value is set, then the system observes an unlimited session time.

While 60 minutes is a good operating baseline for the session, depending on your organization this may vary. For example, in K-12 a 24 hour (1440 minutes) session might be the best setting. Use the best setting for your organization's needs.

Rationale:

Setting a session length allows Chrome OS to not have a user session continuously signed in, thus preventing unauthorized access by someone other than the user.

Impact:

There could be impacts to the user if they are unaware of, or are not actively checking, the session timer. They might be logged out unexpectedly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Maximum user session length**
6. Ensure **Maximum session length** is set to your organization's parameters

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Maximum user session length**
6. Set **Maximum session length** to your organization's parameters
7. Select **Save**





Default Value:

Unset (Unlimited session length)

References:

1. <https://chromeenterprise.google/policies/#SessionLengthLimit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

2.3.1.1.2 (L1) *Ensure 'Custom terms of service' Is Configured (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

If users are not informed of their responsibilities, unapproved activities may occur. Users that are not approved for access may take the lack of a warning banner as implied consent to access.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Custom terms of service**
6. Ensure a **.txt** or **.text** file has been uploaded that contains your organization's custom terms of service

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Custom terms of service**
6. Select **Upload**
7. Select a **.txt** or **.text** file from your local device that contains your organization's custom terms of service
8. Select **Save**

Default Value:

Unset

References:

1. <https://chromeenterprise.google/policies/#TermsOfServiceURL>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.2 Apps and extensions

2.3.1.2.1 (L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Task Manager in ChromeOS allows the user to kill any current processes running.

Rationale:

If the Task Manager is enabled, a user can kill any running task including those that your organization uses to manage the user of the device. Disabling that functionality removes that possibility.

Impact:

If a task is no longer responding, the user would have to turn the device off and back on to kill that task.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **Task manager**
7. Ensure the configuration is set to **Block users from ending processes with the Chrome task manager**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **Task manager**
7. Set to **Block users from ending processes with the Chrome task manager**
8. Select **Save**







Default Value:

Unset (same as enabled)

References:

1. <https://chromeenterprise.google/policies/#TaskManagerEndProcessEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.3.1.2.2 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls extension management settings for Google Chrome, specifically v2 extensions. This policy setting is being sunsetted as Google develops the Manifest v3, but that rollout is currently postponed.

The policy can be configured to:

- Default (0): Default browser behavior
- Disabled (1): Manifest v2 is disabled
- Enabled (2): Manifest v2 is enabled
- Forced Only (3): Manifest v2 is enabled for forced extensions only

Rationale:

Setting this to Forced Only will not allow users to install any additional v2 extensions, and all existing, non-forced, v2 extensions will be disabled.

Impact:

Users that use extensions regularly will have a set of them blocked, which will change their user experience.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Manifest v2 extension availability**
6. Ensure **Configuration** is set to **Enable force-installed manifest v2 extensions on the sign-in screen**

Remediation:







To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Manifest v2 extension availability**
6. Set **Configuration** to **Enable force-installed manifest v2 extensions on the sign-in screen**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ExtensionManifestV2Availability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 <u>Establish and Maintain a Remediation Process</u> Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.3.1.3 Site isolation

2.3.1.3.1 (L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls if every website will load into its own process.

Disabled (0): Doesn't turn off site isolation, but it lets users opt out.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Chrome will load each website in its own process. Even if a site bypasses the same-origin policy, the extra security will help stop the site from stealing your data from another website.

Impact:

If the policy is enabled, each site will run in its own process which will cause the system to use more memory. You might want to look at the **Enable Site Isolation for specified origins** policy setting to get the best of both worlds – isolation and limited impact for users – by using **Enable Site Isolation for specified origins** with a list of the sites you want to isolate.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Site isolation**
6. Ensure **Configuration** is set to **Require Site Isolation for all websites, as well as any origins below**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Site isolation**
6. Set **Configuration** to **Require Site Isolation for all websites, as well as any origins below**
7. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SitePerProcess>
2. <https://www.chromium.org/Home/chromium-security/site-isolation>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.3.1.4 Security

2.3.1.4.1 (L1) Ensure 'Password manager' is Explicitly Configured (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome has a built-in password manager to store passwords for users. Chrome will use local authentication to allow users to gain access to these passwords.

The recommended state for this setting is: Explicitly set to **Enabled** (1) or **Disabled** (0) based on the organization's needs.

NOTE: If you choose to Enable this setting, please review **Disable synchronization of data with Google** and ensure this setting is configured to meet organizational requirements.

Rationale:

The Google Chrome password manager is **Enabled** by default and each organization should review and determine if they want to allow users to store passwords in the Browser. If another solution is used instead of the built-in Chrome option then an organization should configure the setting to **Disabled**.

Impact:

Organizationally dependent.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Password manager**
6. Ensure **Configuration** is set to **Always allow use of password manager** or **Never allow use of password manager**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Password manager**
6. Set **Configuration** to **Always allow use of password manager** or **Never allow use of password manager**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PasswordManagerEnabled>
2. <https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers>
3. <https://pages.nist.gov/800-63-3/sp800-63b.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.4.2 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the WebAuthn API and its interaction with sites that have a broken TLS certificate. It can be configured to either:

- Disabled (0): Do not allow WebAuthn API requests on sites with broken TLS certificates.
- Enabled (1): Allow WebAuthn API requests on sites with broken TLS certificates.

If the value for `AllowWebAuthnWithBrokenTlsCerts` is not changed from the default, it will behave as it is disabled.xempt.

Rationale:

Setting this policy will block the ability to authenticate to any website that does not have a valid TLS certificate since the identity of the site cannot be verified.

Impact:

There should be no user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Devices`
3. Select `Chrome`
4. Select `Settings`
5. Under `User & browser settings`, select `Web Authentication requests on sites with broken TLS certificates`
6. Ensure `Configuration` is set to `Do not allow WebAuthn API requests on sites with broken TLS certificates`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Authentication requests on sites with broken TLS certificates**
6. Set **Configuration** to **Do not allow WebAuthn API requests on sites with broken TLS certificates**
7. Select **Save**





Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#AllowWebAuthnWithBrokenTlsCerts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.1.4.3 (L1) Ensure 'Online revocation checks' is set to 'Do not perform online OCSP/CRL checks' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can reactivate soft-fail, online revocation checks, although they may provide some benefit in most cases.

If this setting is disabled, unsecure online OCSP/CRL checks are no longer performed.

The recommended state for this setting is: **Disabled** (0)

Rationale:

CRLSets are primarily a means by which Chrome can quickly block certificates in emergency situations. As a secondary function they can also contain some number of non-emergency revocations. These latter revocations are obtained by crawling CRLs published by CAs.

Online (i.e. OCSP and CRL) checks are not, by default, performed by Chrome. The underlying system certificate library always performs these checks no matter what Chrome does, so enabling it here is redundant.

An attacker may block OCSP traffic and cause revocation checks to pass in order to cause usage of soft-fail behavior. Furthermore, the browser may leak what website is being accessed and who accesses it to CA servers.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Ensure **Configuration** is set to **Do not perform online OCSP/CRL checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Set **Configuration** to **Do not perform online OCSP/CRL checks**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#EnableOnlineRevocationChecks>
2. <https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3>
3. <https://dev.chromium.org/Home/chromium-security/crlsets>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.4 (L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for Google Chrome to allow legacy or insecure hashes during the TLS handshake. It can be configured to either:

- Disabled (0): **Do Not Allow Insecure Hashes in TLS Handshakes**
- Enabled (1): **Allow Insecure Hashes in TLS Handshakes**

If the value for **InsecureHashesInTLSHandshakesEnabled** is not changed from the default, it will behave as if it is enabled.

Rationale:

Setting this policy to disabled will block Google Chrome from using insecure hashes. Using insecure, or legacy, hashes could allow sensitive data to be exposed.

Impact:

Users would be blocked from visiting sites that do not support more secure hashes.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Insecure hashes in TLS handshakes**
6. Ensure **Configuration** is set to **Do not allow insecure hashes in TLS handshakes**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Insecure hashes in TLS handshakes**
6. Set **Configuration** to **Do not allow insecure hashes in TLS handshakes**
7. Select **Save**






Default Value:

Unset (Allow)

References:

1. <https://chromeenterprise.google/policies/#InsecureHashesInTLSHandshakesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	14.4 <u>Train Workforce on Data Handling Best Practices</u> Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.5 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This configures whether Google Chrome will offer a post-quantum key agreement algorithm in TLS, using the ML-KEM NIST standard, and will protect user traffic from quantum computers when communicating with compatible servers. Enabling a post-quantum key agreement is backwards compatible, so there will be no issue with existing TLS servers.

Rationale:

This will protect user traffic from quantum computer decrypting.

Impact:

There should be no impact on the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Post-quantum TLS**
6. Ensure **Configuration** is set to **Allow post-quantum key agreement in TLS connections**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Post-quantum TLS**
6. Set **Configuration** to **Allow post-quantum key agreement in TLS connections**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PostQuantumKeyAgreementEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.1.4.6 (L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **Lock screen PIN** is a secure and convenient alternative for day-to-day use. Its security relies on the underlying hardware and software design of ChromeOS to protect against brute-force attacks and ensure that it cannot be used to compromise the user's broader Google Account.

Rationale:

The **Lock screen PIN** is a security feature designed to encourage frequent use of the lock screen by offering a simple, convenient way to unlock the device. Its security rationale is based on the idea that user convenience leads to better security habits. While the PIN has lower entropy than a full password, its security is reinforced by hardware-based protections that prevent brute-force attacks. It acts as a local credential to unlock encrypted user data, protecting against opportunistic theft and snooping, without compromising the user's main Google Account. The system is a secure and user-friendly compromise that balances convenience with robust protection.

Impact:

Allowing no weak PINs and a minimum length of 6 creates a minor, one-time inconvenience for the user in the name of significantly enhanced device security. The user must adapt to a more complex PIN, but the benefit is a much stronger defense against both opportunistic and targeted attacks on their local device data.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security** select **Users & browsers**
6. Select **Lock screen PIN**
7. Ensure the configuration is set to **Do not allow users to set a weak PIN**
8. Ensure the **Minimum PIN length** is set to 6 or greater

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security** select **Users & browsers**
6. Select **Lock screen PIN**
7. Set the **Configuration** to **Do not allow users to set a weak PIN**
8. Set **Minimum PIN length** to 6 or greater
9. Select **Save**




Default Value:

Unset (no minimum PIN length and Allow users to set a weak PIN, but show a warning)

References:

1. <https://chromeenterprise.google/policies/#PinUnlockMaximumLength>
2. <https://chromeenterprise.google/policies/#PinUnlockMinimumLength>
3. <https://chromeenterprise.google/policies/#PinUnlockWeakPinsAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.7 (L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **PIN auto-submit** setting is a convenience feature that unlocks the device as soon as the correct PIN is typed, without needing to press Enter.

Rationale:

By removing the final manual submission step, it can create a slightly higher risk of exposure to "shoulder surfing" and therefore should be used with a strong PIN and an awareness of the physical environment.

Impact:

There is a minimal impact on the user requiring them to submit the PIN themselves (hitting the enter key) instead of the OS recognizing it as soon as it is typed.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security** select **Users & browsers**
6. Select **PIN auto-submit**
7. Ensure the configuration is set to **Disable PIN auto-submit on the lock and login screen**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security** select **Users & browsers**
6. Select **PIN auto-submit**
7. Set the **Configuration** to **Disable PIN auto-submit on the lock and login screen**
8. Select **Save**

Default Value:

Unset

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.8 (L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Specifies whether the user may open pages in Incognito mode in Google Chrome. The possible values are:

- Incognito mode available (0 - Same as Disabled))
- Incognito mode disabled (1)
- Incognito mode forced (2)

The recommended state for this setting is: Enabled: Incognito mode disabled (1)

Rationale:

Incognito mode in Chrome gives you the choice to browse the internet without your activity being saved to your browser or device.

Allowing users to use the browser without any information being saved can hide evidence of malicious behaviors. This information may be important for a computer investigation, and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Users will not be able to initiate Incognito mode for Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Incognito mode
6. Ensure Configuration is set to Disallow incognito mode

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Incognito mode**
6. Set **Configuration** to **Disallow incognito mode**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#IncognitoModeAvailability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.9 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome is configured to save the browser history.

The recommended state for this setting is: **Always save browser history**

NOTE: This setting will preserve browsing history that could contain a user's personal browsing history. Please make sure that this setting is in compliance with organizational policies.

Rationale:

Browser history shall be saved as it may contain indicators of compromise.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser history**
6. Ensure **Configuration** is set to **Always save browser history**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser history**
6. Set **Configuration** to **Always save browser history**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change).

References:

1. <https://chromeenterprise.google/policies/#SavingBrowserHistoryDisabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

2.3.1.4.10 (L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can delete the browser and download history using the clear browsing data menu.

The recommended state for this setting is: **Disabled** (0)

NOTE: Even when this setting is disabled, the browsing and download history aren't guaranteed to be retained. Users can edit or delete the history database files directly, and the browser itself may remove (based on expiration period) or archive any or all history items at any time.

Rationale:

If users can delete websites they have visited or files they have downloaded, it will be easier for them to hide evidence that they have visited unauthorized or malicious sites.

Impact:

If this setting is disabled, browsing and download history cannot be deleted by using the clear browsing data menu.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clear browser history**
6. Ensure **Configuration** is set to **Do not allow clearing history in settings menu**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clear browser history**
6. Set **Configuration** to **Do not allow clearing history in settings menu**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowDeletingBrowserHistory>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.4.11 (L2) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome performs revocation checking for server certificates that successfully validate and are signed by locally-installed CA certificates. If Google Chrome is unable to obtain revocation status information, such certificates will be treated as revoked ('hard-fail').

Disabled: Google Chrome uses existing online revocation-checking settings.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Certificates shall always be validated.

Impact:

A revocation check will be performed for server certificates that successfully validate and are signed by locally-installed CA certificates. if the OCSP server goes down, then this will hard-fail and prevent browsing to those sites.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Ensure **Configuration** is set to **Perform online OCSP/CRL checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Online revocation checks**
6. Set **Configuration** to **Perform online OCSP/CRL checks**
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#RequireOnlineRevocationChecksForLocalAnchors>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.12 (L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome supports tracking a user's physical location using GPS, data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP.

- Disabled (0, same as 3)
- Allow sites to track the users' physical location (1)
- Do not allow any site to track the users' physical location (2)
- Ask whenever a site wants to track the users' physical location (3)

The recommended state for this setting is: Enabled with a value Do not allow any site to track the users' physical location (2)

Rationale:

From a privacy point of view it is not desirable to submit indicators regarding the location of the device, since the processing of this information cannot be determined. Furthermore, this may leak information about the network infrastructure around the device.

Impact:

If this setting is disabled, chrome will no longer send data about nearby Wi-Fi access points or cellular signal sites/towers (even if you're not using them), and your computer's IP address to Google.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Geolocation
6. Ensure Configuration is set to Do not allow sites to detect users' geolocation

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Geolocation**
6. Set **Configuration** to **Do not allow sites to detect users' geolocation**
7. Select **Save**



Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultGeolocationSetting>
2. <https://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-24.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.4.13 (L1) Ensure 'Google online login frequency' Is Set to '1' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

During login, Google ChromeOS can authenticate against an online server or by using an offline cached password. This configuration sets the frequency of forced online sign-ins on the login screen for users signing into their ChromeOS device without SAML single sign-on (SSO).

Rationale:

Each time users sign out after the set frequency period, they must go through the online sign-in flow.

When users sign in online, they use the Google identity service. By forcing users to regularly sign in, you provide additional security for organizations that require 2-Factor Authentication or Multi-Factor Authentication.

Impact:

This may cause users to have to log into the OS more frequently.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Select **Google online login frequency**
7. Ensure **Force online login flow for Google accounts** is set to **1**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Select **Google online login frequency**
7. Set to **Force online login flow for Google accounts** is set to **1**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#GaiaOfflineSigninTimeLimitDays>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.1.4.14 (L1) Ensure 'Google online unlock frequency' is set to '1' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This configuration sets the frequency of forced online sign-ins on the lock screen for users unlocking their ChromeOS device without SAML single sign-on (SSO).

Rationale:

Each time the ChromeOS device locks, the must go through the online unlock flow after a set frequency.

When users sign in online, they use the Google identity service. By forcing users to regularly sign in, you provide additional security for organizations that require 2-Factor Authentication or Multi-Factor Authentication.

Impact:

This may cause users to have to log into the OS more frequently to unlock the device.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **Google online unlock frequency**
7. Ensure **Force online unlock flow for Google accounts** is set to **1**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **Google online unlock frequency**
7. Set to **Force online unlock flow for Google accounts** is set to **1**
8. Select **Save**




Default Value:

Unset (not enforcing online authentication on the lock screen)

References:

1. <https://chromeenterprise.google/policies/#GaiaLockScreenOfflineSigninTimeLimitDays>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.15 (L1) Ensure 'SAML single sign-on login frequency is set to 'Every day' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy is for organizations that are using SAML single sign-on (SSO). This configuration sets the frequency of forced online sign-ins on the login screen for users signing into their ChromeOS device with SAML single sign-on (SSO).

Rationale:

Each time users sign out after the set frequency period, they must go through the online sign-in flow.

When users sign in online, they use their SAML SSO credentials. By forcing users to regularly sign in, you provide additional security for organizations that require 2-Factor Authentication or Multi-Factor Authentication.

Impact:

This may cause users to have to log into the OS more frequently.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **SAML single sign-on login frequency**
7. Ensure **Configuration** is set to **Every day**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **SAML single sign-on login frequency**
7. Set to **Configuration** is set to **Every day**
8. Select **Save**




Default Value:

Unset (14 days)

References:

1. <https://chromeenterprise.google/policies/#SAMLOfflineSignInTimeLimit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.1.4.16 (L1) Ensure 'SAML single sign-on unlock frequency is set to '1' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This configuration sets the frequency of forced online sign-ins on the lock screen for users unlocking their ChromeOS device with SAML single sign-on (SSO).

Rationale:

Each time the ChromeOS device locks, the must go through the online unlock flow after a set frequency.

When users sign in online, they use their SAML SSO credentials. By forcing users to regularly sign in, you provide additional security for organizations that require 2-Factor Authentication or Multi-Factor Authentication.

Impact:

This may cause users to have to log into the OS more frequently to unlock the device.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **SAML single sign-on unlock frequency**
7. Ensure **Force online unlock for SAML based Sign-On accounts** is set to **1**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Settings** select **Users & browsers**
6. Under **Security** select **SAML single sign-on unlock frequency**
7. Set to **Force online unlock for SAML based Sign-On accounts** is set to **1**
8. Select **Save**




Default Value:

Unset (online authentication will not be enforced)

References:

1. <https://chromeenterprise.google/policies/#SamlLockScreenOfflineSignInTimeLimitDays>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.17 (L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can specify URLs/hostnames for which Certificate Transparency will not be enforced. If this setting is disabled, no URLs are excluded from Certificate Transparency requirements.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Certificates that are required to be disclosed via Certificate Transparency shall be treated for all URLs as untrusted if they are not disclosed according to the Certificate Transparency policy.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allowed certificate transparency URLs**
6. Ensure **Allowed certificate transparency URLs** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allowed certificate transparency URLs**
6. Remove all URLs from **Allowed certificate transparency URLs**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CertificateTransparencyEnforcementDisabledForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.18 (L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can exclude certificates by their subjectPublicKeyInfo hashes from enforcing Certificate Transparency requirements. If this setting is disabled, no certificates are excluded from Certificate Transparency requirements.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Certificate Transparency requirements shall be enforced for all certificates.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency CA allowlist**
6. Ensure **Certificate transparency CA allowlist** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency CA allowlist**
6. Remove all CAs from **Certificate transparency CA allowlist**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CertificateTransparencyEnforcementDisabledForCas>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.19 (L1) Ensure 'Certificate transparency legacy CA allowlist' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can disable the enforcing of Certificate Transparency requirements for a list of Legacy Certificate Authorities.

If this setting is disabled, certificates not properly publicly disclosed as required by Certificate Transparency are untrusted.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Legacy Certificate Authorities shall follow the Certificate Transparency policy.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency legacy CA allowlist**
6. Ensure **Certificate transparency legacy CA allowlist** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Certificate transparency legacy CA allowlist**
6. Remove all legacy CAs from **Certificate transparency legacy CA allowlist**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#CertificateTransparencyEnforcementDisabledForLegacyCas>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.20 (L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy allows a user to import or remove CA certificates in Certificate Manager.

The settings for **User management of installed CA certificates** are:

- Allow users to manage all certificates — This is the default. Users can edit trust settings for all CA certificates, remove user-imported certificates, and import certificates.
- Allow users to manage user certificates — Users can manage only user-imported certificates, but they can't change trust settings for built-in certificates.
- Disallow users from managing certificates — Users can view CA certificates, but they can't manage them.

Rationale:

Granting a user the ability to remove CA certificates could allow them to change the trust settings of built-in CA certificates. Allowing users to import their own CA certificates could allow a malicious CA certificate to be trusted.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **User management of installed CA certificates**
7. Ensure the configuration is set to **Disallow users from managing certificates**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **User management of installed CA certificates**
7. Set to **Disallow users from managing certificates**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#CACertificateManagementAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.21 (L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy allows a user to import or remove certificates in Certificate Manager.

The settings for **User management of installed certificates** are:

- Allow users to manage all certificates — This is the default. Users can edit trust settings for all certificates, remove user-imported certificates, and import certificates.
- Allow users to manage user certificates — Users can manage only user-imported certificates, but they can't change trust settings for built-in certificates.
- Disallow users from managing certificates — Users can view certificates, but they can't manage them.

Rationale:

Granting a user the ability to remove certificates could allow them to change the trust settings of built-in certificates. Allowing users to import their own certificates could allow a malicious certificate to be trusted.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **User management of installed client certificates**
7. Ensure the configuration is set to **Disallow users from managing certificates**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Apps and extensions** select **Users & browsers**
6. Select **User management of installed client certificates**
7. Set to **Disallow users from managing certificates**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ClientCertificateManagementAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.22 (L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls the ability for Google Chrome to verify if any entered credentials were part of a leak. If a user's credentials are compromised, the user will be alerted. The password is not stored on Google's servers, unless Password Sync is enabled, and is encrypted with a secret key known only to your device. To find out more on how Google protects your password, see their support article [How Chrome protects your passwords](#).

Note: This setting has no effect if **Safe Browsing** is not enabled.

Rationale:

Users should be aware if any of their credentials have been compromised or leaked.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Enable leak detection for entered credentials**
6. Ensure **Configuration** is set to **Users enrolled in the Advanced Protection program will receive extra protections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Enable leak detection for entered credentials**
6. Set **Configuration** to **Users enrolled in the Advanced Protection program will receive extra protections**
7. Select **Save**






Default Value:

Unset (Allow the user to decide)

References:

1. <https://chromeenterprise.google/policies/#PasswordLeakDetectionEnabled>
2. <https://support.google.com/chrome/a/answer/13597868?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.4.23 (L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome will show a warning that appears when Google Chrome is running on a computer or operating system that is no longer supported.

The recommended state for this setting is: **Disabled** (0)

Rationale:

The user shall be informed if the used software is no longer supported.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Unsupported system warning**
6. Ensure **Configuration** is set to **Allow Chrome to display warnings when running on an unsupported system**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Unsupported system warning**
6. Set **Configuration** to **Allow Chrome to display warnings when running on an unsupported system**
7. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SuppressUnsupportedOSWarning>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.3.1.4.24 (L2) Ensure Advanced Protection Program is configured (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enable Google's Advanced Protection Platform for all users and prevent the use of security codes where applicable.

Rationale:

Sophisticated phishing tactics can trick the most savvy users into giving their sign-in credentials to attackers. Advanced Protection requires you to use a security key, which is a hardware device or special software on your phone used to verify your identity, to sign in to your Google Account. Unauthorized users won't be able to sign in without your security key, even if they have your username and password.

The Advanced Protection Program includes a curated group of high-security policies that are applied to enrolled accounts. Additional policies may be added to the Advanced Protection Program to ensure the protections are current.

Advanced Protection allows you to apply all of these protections at once, and override similar settings you may have configured manually. These policies include:

- Strong authentication with security keys
- Use of security codes with security keys (as needed)
- Restrictions on third-party access to account data
- Deep Gmail scans
- Google Safe Browsing protections in Chrome (when users are signed into Chrome using the same identity as their Advanced Protection Program identity)
- Account recovery through admin

Impact:

User Impact

- You need your security key when you sign in for the first time on a computer, browser, or device. If you stay signed in, you may not be asked to use your security key the next time you log in.
- Limits third-party app access to your data, puts stronger checks on suspicious downloads, and tightens account recovery security to help prevent unauthorized access.

Security Keys - 2 Required

- Android: With an Android 7.0+ phone, you can enroll in a few taps by registering your phone's built-in security key.
- iPhone: If you have an iPhone running iOS 10.0+, install the **Google Smart Lock** app to register your security key first, then enroll.
- Two security keys are required for added assurance. If one key is lost or damaged, users can use the second key to regain account access.

Third-Party IdP

- You can use the Advanced Protection Program with accounts that federate from an IdP using SAML. When users with these accounts enroll in the Advanced Protection Program, we'll require security key use after the user signs in on the IdP. Note that SAML users can select Remember the device to avoid challenges on a browser or device.

Security Codes

- Before allowing users to generate security codes, carefully evaluate if your organization needs them. Using security keys with security codes increases the risk of phishing. However, if your organization has important workflows where security keys can't be used directly, enabling security codes for those situations may help improve your security posture overall.

Using 'Sign in with Google' with other apps and services

- You can still sign into apps and services with Google. If they request access to your Gmail or Drive data, access is denied.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Security**
3. Select **Advanced Protection Program**
4. Under **Enrollment - Allow users to enroll in the Advanced Protection Program**, ensure **Enable user enrollment** is **selected** for the desired organizational unit or group
5. Under **Security Codes**, ensure **Do not allow users to generate security codes** is **selected** for the desired organizational unit or group

Remediation:





To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Security**
3. Select **Advanced Protection Program**
4. Under **Enrollment - Allow users to enroll in the Advanced Protection Program**, set **Enable user enrollment** to **selected** for the desired organizational unit or group
5. Under **Security Codes**, set **Do not allow users to generate security codes** to **selected** for the desired organizational unit or group
6. Select **Save**

Default Value:

- **Allow users to enroll in the Advanced Protection Platform** is **selected**
- **Security codes** is **Allow security codes without remote access**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

2.3.1.4.25 (L1) *Ensure 'Override insecure origin restrictions' is Not Set (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can use a list of origins (URLs) or hostname patterns (such as "*.example.com") for which security restrictions on insecure origins will not apply and are prevented from being labeled as "Not Secure" in the omnibox.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Insecure contexts shall always be labeled as insecure.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Override insecure origin restrictions**
6. Ensure **Origin or hostname patterns to ignore insecure origins security restrictions** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Override insecure origin restrictions**
6. Remove all hostnames from **Origin or hostname patterns to ignore insecure origins security restrictions**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#OverrideSecurityRestrictionsOnInsecureOrigin>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.4.26 (L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users may use remote debugging.

The recommended state for this setting is: **Do not allow use of the remote debugging**.

Rationale:

Disabling remote debugging enhances security and protects applications from unauthorized access. Some attack tools can exploit this feature to extract information, or to insert malicious code.

Impact:

Users will not be able access the remote debugging feature in Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow remote debugging**
6. Ensure **Configuration** is set to **Do not allow use of the remote debugging**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow remote debugging**
6. Set **Configuration** to **Do not allow use of the remote debugging**
7. Select **Save**







Default Value:

Enabled. (Users may use remote debugging by specifying --remote-debug-port and --remote-debugging-pipe command line switches.)

Additional Information:

I copied/adjusted this rule from [MS Edge, rule 1.41](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 <u>Establish and Maintain a Remediation Process</u> Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.1.4.27 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the defaults for using Encrypted ClientHello (ECH). ECH is an extension to TLS and encrypts the initial handshake with a website that can only be decrypted by that website. Google Chrome may, or may not, use ECH based on 3 factors: server support, HTTPS DNS record availability, or rollout status. It can be configured to either:

- Disabled (0): **Disable the TLS Encrypted ClientHello experiment**
- Enabled (1): **Enable the TLS Encrypted ClientHello experiment**

If the value for **EncryptedClientHelloEnabled** is not changed from the default, it will behave as if it is enabled.

Rationale:

Previously all handshakes were in the open and could expose sensitive information, like the name of the website to which you are connecting. Setting this policy will allow Google Chrome to use an encrypted hello, or handshake, with a website where it is supported, thus not exposing sensitive information.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **TLS encrypted ClientHello**
6. Ensure **Configuration** is set to **Enable the TLS Encrypted ClientHello experiment**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **TLS encrypted ClientHello**
6. Set **Configuration** to **Enable the TLS Encrypted ClientHello experiment**
7. Select **Save**





Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#EncryptedClientHelloEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.1.4.28 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:

- Disabled (0): Scripts for workers (Web Workers, Service Workers, etc.) use lax MIME type checking. Worker scripts with legacy MIME types, like text/ascii, will work.
- Enabled (1): Scripts for workers (Web Workers, Service Workers, etc.) require a JavaScript MIME type, like text/javascript. Worker scripts with legacy MIME types, like text/ascii, will be rejected.

If the value for `StrictMimetypeCheckForWorkerScriptsEnabled` is not changed from the default, it will behave as if it is enabled.

Rationale:

Setting this policy will require worker scripts to use more secure and strict JavaScript MIME types and ones with legacy MIME Types will be rejected.

Impact:

This should have no impact on users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Strict MIME type checking for worker scripts**
6. Ensure **Configuration** is set to **Require a JavaScript MIME type for worker scripts**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Strict MIME type checking for worker scripts**
6. Set **Configuration** to **Require a JavaScript MIME type for worker scripts**
7. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#StrictMimetypeCheckForWorkerScriptsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.8 Implement Application Whitelisting of Libraries The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			●

2.3.1.4.29 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for `showOpenFilePicker()`, `showSaveFilePicker()`, and `showDirectoryPicker()` web APIs to be called without user interaction.

If the value for `FileOrDirectoryPickerWithoutGestureAllowedForOrigins` is not changed from the default, it will behave as if it is disabled.

Rationale:

Setting this policy would allow the URLs selected to call the `showOpenFilePicker()`, `showSaveFilePicker()`, and `showDirectoryPicker()` web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

Impact:

Disabling this policy should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File/directory picker without user gesture**
6. Ensure **Allow file or directory picker APIs to be called without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File/directory picker without user gesture**
6. Remove all URLs from **Allow file or directory picker APIs to be called without prior user gesture**
7. Select **Save**







Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#FileOrDirectoryPickerWithoutGestureAllowedForOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.3.1.4.30 (L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for `getDisplayMedia()` web API to be called without user interaction based on sites that are configured in this policy. By default, no site can call the `getDisplayMedia()` API for screen capture without a prior user gesture.

Rationale:

Setting this policy would allow the URLs selected to call the `getDisplayMedia()` web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

Impact:

Disabling this policy should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Media picker without user gesture**
6. Ensure **Allow screen capture without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Security**, select **Media picker without user gesture**
6. Remove all URLs from **Allow screen capture without prior user gesture**
7. Select **Save**

Default Value:

Unset (disabled)

References:

1. <https://chromeenterprise.google/policies/#ScreenCaptureWithoutGestureAllowedForOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.5 Remote Access

2.3.1.5.1 (L2) *Ensure 'Remote access clients' Is Configured (Manual)*

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The policy imposes what client domain names have access to remotely connect to the ChromeOS device. If the policy is unset then any client from any domain can connect to the ChromeOS device.

Rationale:

In order to stop remote access by any client on any domain, this policy should be configured to your organization's domains that need to remotely access your ChromeOS devices.

Impact:

There should be no impact to the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Remote Access**, select **Remote access clients**
6. Ensure **Remote access client domain** is set to your organization's required domain(s)

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Remote Access**, select **Remote access clients**
6. Set **Remote access client domain** to your organization's required domain(s)
7. Select **Save**






Default Value:

Unset, any client domain may connect to the host remotely.

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostClientDomainList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 <u>Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure</u> Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.			
v7	12.1 <u>Maintain an Inventory of Network Boundaries</u> Maintain an up-to-date inventory of all of the organization's network boundaries.			

2.3.1.5.2 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Chrome allows the configuration of a list of domains that are allowed to access the user's system. When enabled, remote systems can only connect if they are one of the specified domains listed.

Setting this to an empty list (Disabled) allows remote systems from any domain to connect to this user's system.

The recommended state for this setting is: **Enabled** (1) and at least one domain set

NOTE: The list of domains is organization specific.

Rationale:

Remote assistance connections shall be restricted.

Impact:

If this setting is enabled, only systems from the specified domains can connect to the user's system.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote access hosts**
6. Ensure **Remote access host domain** is set to your organization's required domain

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote access hosts**
6. Set **Remote access host domain** to your organization's required domain
7. Select **Save**




Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostClientDomainList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.1.5.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome allows the use of relay servers when clients are trying to connect to this machine and a direct connection is not available.

- **Disable** (0): The use of relay servers by the remote access host is not allowed
- **Enabled** (1): The use of relay servers by the remote access host is allowed

The recommended state for this setting is: **Disabled** (0)

Rationale:

Relay servers shall not be used to circumvent firewall restrictions.

Impact:

If this setting is disabled, remote clients can not use relay servers to connect to this machine.

NOTE: Setting this to Disabled doesn't turn remote access off, but only allows connections from the same network (not NAT traversal or relay).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Ensure **Configuration** is set to **Disable the use of relay servers**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Firewall traversal**
6. Set **Configuration** to **Disable the use of relay servers**
7. Select **Save**




Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRelayedConnection>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.1.5.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This is a setting for Chrome Remote desktop. If this setting is Disabled, the remote access host service cannot be started or configured to accept incoming connections.

- **Disabled** (0): Prevent remote access connections to this machine
- **Enabled** (1): Allow remote access connections to this machine

The recommended state for this setting is: **Disabled** (0)

Rationale:

Only approved remote access systems should be used.

NOTE: If Chrome Remote Desktop is approved and required for use, then this setting can be ignored.

Impact:

This setting will disable Chrome Remote Desktop. In general, Chrome Remote Desktop is not used by most businesses, so disabling it should have no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote support connections**
6. Ensure **Configuration** is set to **Prevent remote support connections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Remote support connections**
6. Set **Configuration** to **Prevent remote support connections**
7. Select **Save**




Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRemoteAccessConnections>
2. <https://remotedesktop.google.com/?pli=1>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.1.6 Session Settings

2.3.1.6.1 (L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **Show sign-out button in tray** policy controls whether a sign-out button is in the system tray while the screen is not locked and the session is active.

Rationale:

Enabling the sign-out button in the system tray would allow a user to quickly logout of a session in a situation where there may be malicious actors trying to 'shoulder-surf' or to capture data from the user's screen.

Impact:

This would have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Session settings**, select **Show sign-out button in tray**
6. Ensure **Show sign-out button in tray** is set to **Show sign-out button in tray**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Session settings**, select **Show sign-out button in tray**
6. Set **Show sign-out button in tray** to **Show sign-out button in tray**
7. Select **Save**




Default Value:

Unset, no sign-out button.

References:

1. <https://chromeenterprise.google/policies/#ShowLogoutButtonInTray>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.7 Network

2.3.1.7.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers the functionality to configure the proxy settings by automatic discovery using WPAD (Web Proxy Auto-Discovery Protocol). Setting this configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified from the command line.

Disabled (0): Lets users choose their proxy settings.

The recommended state for this setting is: **Enabled** and the value of **ProxyMode** is not set to **auto_detect**

Rationale:

Attackers may abuse the WPAD auto-config functionality to supply computers with a PAC file that specifies a rogue web proxy under their control.

Impact:

If the policy is enabled, the proxy configuration will no longer be discovered using WPAD.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Proxy mode**
6. Ensure **Configuration** is not set to **Always auto detect the proxy**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Proxy mode**
6. Set **Configuration** to a setting other than **Always auto detect the proxy**
7. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#ProxySettings>
2. http://www.ptsecurity.com/download/wpad_weakness_en.pdf
3. <https://www.blackhat.com/us-16/briefings.html#crippling-https-with-unholy-pac>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●
v7	12.9 Deploy Application Layer Filtering Proxy Server Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●

2.3.1.7.2 (L2) *Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Automated)*

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy configures the ability for Google ChromeOS to bypass any proxy for captive portal authentication.

If enabled, this causes authentication webpages – starting from the captive portal sign-in page until Chrome detects a successful internet connection – to open in a separate window and ignore all policy settings and restrictions for the current user.

If disabled, this means any captive portal authentication pages are shown in a new browser tab that uses the current user's proxy settings.

This policy only takes effect if a proxy is set up (by policy, extension, or the user in `chrome://settings`).

Rationale:

Enabling captive portal sites to bypass proxy settings could grant access to the system from a malicious (or misconfigured) captive portal site. Setting the policy to disabled forces all sites, including captive portal sites, to use the configured proxy settings.

Impact:

This may impact a user's access to certain captive portal sites that do not work with the configured proxy server.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Network**
6. Ensure **Ignore proxy on captive portals** is set to **Keep policies for captive portal pages**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **General**, select **Network**
6. Set **Ignore proxy on captive portals** to **Keep policies for captive portal pages**
7. Select **Save**





Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#CaptivePortalAuthenticationIgnoresProxy>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	15.1 <u>Maintain an Inventory of Authorized Wireless Access Points</u> Maintain an inventory of authorized wireless access points connected to the wired network.			

2.3.1.7.3 (L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Specifies which HTTP authentication schemes are supported by Google Chrome.

Disabled (0): Allows all supported authentication schemes.

The recommended state for this setting is: **Enabled** with the value of **ntlm, negotiate**

Rationale:

Possible values are 'basic', 'digest', 'ntlm' and 'negotiate'. Basic and Digest authentication do not provide sufficient security and can lead to submission of user passwords in plaintext or minimal protection (Integrated Authentication is supported for negotiate and ntlm challenges only).

Impact:

If some legacy application(s) or website(s) required insecure authentication mechanisms they will not work correctly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Supported authentication schemes**
6. Ensure **Configuration** is set to **NTLM** and **Negotiate**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Supported authentication schemes**
6. Set **Configuration** to **NTLM** and **Negotiate**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AuthSchemes>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

2.3.1.7.4 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls whether a user is able to proceed to a webpage when an invalid SSL certificate warning has occurred.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Sites protected by SSL should always be recognized as valid in the web browser. Allowing a user to make the decision as to whether there appears to be an invalid certificate could open an organization up to users visiting a site that is otherwise not secure and/or malicious in nature.

Impact:

Users will not be able to click past the invalid certificate error to view the website.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SSL error override**
6. Ensure **Configuration** is set to **Block users from clicking through SSL warnings**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SSL error override**
6. Set **Configuration** to **Block users from clicking through SSL warnings**
7. Select **Save**





Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SSLErrorOverrideAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.7.5 (L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting specifies a list of URLs or patterns for which local IP addresses will be exposed by WebRTC.

The recommended state for this setting is: **Disabled** (0)

NOTE: This setting, if Enabled, weakens the protection of local IPs if needed by administrators.

Rationale:

Enabling this setting and allowing exposure of IP addresses can allow an attacker to gather information about the internal network that could potentially be utilized to breach and traverse a network.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebRTC ICE candidate URLs for local IPs**
6. Ensure **URLs for which local IPs are exposed in WebRTC ICE candidates** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebRTC ICE candidate URLs for local IPs**
6. Remove all URLs from **URLs for which local IPs are exposed in WebRTC ICE candidates**
7. Select **Save**






Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#WebRtcLocalIpsAllowedUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.7.6 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This controls the mode of the DNS-over-HTTPS resolver. Please note that this setting will only set the default mode for each query. The mode may be overridden for special types of queries, such as requests to resolve a DNS-over-HTTPS server hostname.

- **Disable DNS-over-HTTPS** (off)
- **Enable DNS-over-HTTPS with insecure fallback** (automatic) - Enable DNS-over-HTTPS queries first if a DNS-over-HTTPS server is available and may fallback to sending insecure queries on error.
- **Enable DNS-over-HTTPS without insecure fallback** (secure) - Only send DNS-over-HTTPS queries and will fail to resolve on error.

The recommended state for this setting is: **Enabled** with a value of **Enable DNS-over-HTTPS without insecure fallback** (secure)

Note: When enabling this policy, it is recommended to also configure the **DnsOverHttpsTemplates** policy so that the URI templates are set. You can find out more information on the [DnsOverHttpsTemplates enterprise policy site](#).

Rationale:

DNS over HTTPS (DOH) has a couple primary benefits:

1. Encrypting DNS name resolution traffic helps to hide your online activities, since DoH hides the name resolution requests from the ISP and from anyone listening on intermediary networks.
2. DoH also helps to prevent DNS spoofing and man-in-the-middle (MitM) attacks.

Impact:

Not all DNS providers support DOH, so choice is limited. Also, Enterprises sometimes monitor DNS requests to block access to malicious or inappropriate sites. DNS monitoring can also sometimes be used to detect malware attempting to "phone home." Because DoH encrypts name resolution requests, it can create a security monitoring blind spot.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS over HTTPS**
6. Ensure **Configuration** is set to **Enable DNS-over-HTTPS without insecure fallback**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS over HTTPS**
6. Set **Configuration** to **Enable DNS-over-HTTPS without insecure fallback**
7. Select **Save**








Default Value:

Unset (Same as Enable DNS-over-HTTPS with insecure fallback – automatic). If any policy is set, either through being domain-joined or active policy with cloud management (or profile lists), then it sometimes reverts to Disable DNS-over-HTTPS and users can't change it.

References:

1. <https://chromeenterprise.google/policies/#DnsOverHttpsMode>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	14.4 <u>Train Workforce on Data Handling Best Practices</u> Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.1.7.7 (L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether third-party sub-content can open a HTTP Basic Auth dialog and is typically disabled.

The recommended state for this setting is: **Block cross-origin authentication**

Rationale:

This setting is typically disabled to help combat phishing attempts.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cross-origin authentication**
6. Ensure **Specify whether third-party sub-content on a page is allowed to pop-up an HTTP basic authentication dialog box.** is set to **Block cross-origin authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cross-origin authentication**
6. Set **Specify whether third-party sub-content on a page is allowed to pop-up an HTTP basic authentication dialog box.** to **Block cross-origin authentication**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowCrossOriginAuthPrompt>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.7.8 (L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether HTTP auth credentials may be automatically used in the context of another web site visited in Google Chrome.

The recommended state for this setting is: **Disabled** (0)

NOTE: This setting is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future.

Rationale:

Allowing HTTP auth credentials to be shared without the user's consent could lead to a user sharing sensitive information without their knowledge. Enabling this setting could also lead to some types of cross-site attacks that would allow users to be tracked across sites without the use of cookies.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Globally scoped HTTP authentication cache**
6. Ensure **Configuration** is set to **Block cross-origin authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Globally scoped HTTP authentication cache**
6. Set **Configuration** to **HTTP authentication credentials are scoped to top-level sites**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#GloballyScopeHTTPAuthCacheEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.7.9 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows a list of names to be specified that will be exempt from HTTP Strict Transport Security (HSTS) policy checks, then potentially upgraded from http:// to https://.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Allowing hostnames to be exempt from HSTS checks could allow for protocol downgrade attacks and cookie hijackings.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HSTS policy bypass list**
6. Ensure **List of hostnames that will bypass the HSTS policy check** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HSTS policy bypass list**
6. Remove all hostnames from **List of hostnames that will bypass the HSTS policy check**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#HSTSPolicyBypassList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.7.10 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines whether a local switch is configured for DNS interception checks. These checks attempt to discover if the browser is behind a proxy that redirects unknown host names.

The recommended state for this setting is: **Enabled** (1)

NOTE: This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on startup and each DNS configuration change.

Rationale:

Disabling these checks could potentially allow DNS hijacking and poisoning.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS interception checks enabled**
6. Ensure **Configuration** is set to **Perform DNS interception checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **DNS interception checks enabled**
6. Set **Configuration** to **Perform DNS interception checks**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DNSInterceptionChecksEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.7 Remediate Detected Vulnerabilities Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

2.3.1.7.11 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows administrators to list specific sites that will not be upgraded to HTTPS and will not show an error interstitial if **HTTPS-First Mode** is enabled.

Note: Wildcards (*, [*], etc.) are not allowed in the URL listings.

Rationale:

Setting this policy allows organizations to maintain access to servers that do not support HTTPS without having to disable HTTPS-First mode or HTTPS Upgrades.

Impact:

This should not have an impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HTTP Allowlist**
6. Ensure **Allowed HTTP URLs** is set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **HTTP Allowlist**
6. Set **Allowed HTTP URLs** to your organization's requirements
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#HttpAllowlist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.5 Integrate Software and Hardware Asset Inventories The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●

2.3.1.7.12 (L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:

- Disabled (0): **Disable HTTPS Upgrades**
- Enabled (1): **HTTPS Upgrades may be applied depending on feature launch status**

If the value for **HttpsUpgradesEnabled** is not changed from the default, it will behave as if it is enabled.

Rationale:

Enabling this setting will upgrade the connection to a site from HTTP to HTTPS where available, verifying the identity of the site visited.

Impact:

This should have no impact on the user.

Note: If there are internal sites/servers that use HTTP only, set those in the policy **HttpAllowlist**

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Automatic HTTPS upgrades**
6. Ensure **Configuration** is set to **Allow HTTPS upgrades**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Automatic HTTPS upgrades**
6. Set **Configuration** to **Allow HTTPS upgrades**
7. Select **Save**






Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#HttpsUpgradesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.8 Content

2.3.1.8.1 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting ensures that web search results with Google are performed with SafeSearch set to always active. Disabled means SafeSearch in Google Search is not enforced.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are more prone to malicious content, including spyware, adware, and viruses.

Impact:

Users search results will be filtered and content such as adult text, videos, and images will not be shown.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSearch and Restricted Mode**
6. Ensure **Configuration** is set to **Always use Safe Search for Google Web Search queries**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSearch and Restricted Mode**
6. Set **Configuration** to **Always use Safe Search for Google Web Search queries**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ForceGoogleSafeSearch>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.8.2 (L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls whether Google Chrome can use screen-share APIs, including web-based online meetings, video, or screen sharing.

The recommended state for this setting is **Do not allow sites to prompt the user to share a video stream of their screen**.

NOTE: This setting is not considered (and a site will be allowed to use screen-share APIs) if the site matches an origin pattern in any of the following other settings: *ScreenCaptureAllowedByOrigins*, *WindowCaptureAllowedByOrigins*, *TabCaptureAllowedByOrigins*, *SameOriginTabCaptureAllowedByOrigins*.

Rationale:

Allowing screen-share APIs within Google Chrome could potentially allow for sensitive data to be shared via screen captures.

Impact:

Users will be unable to utilize APIs which support web-based meetings (video conferencing screen sharing), video, and screen capture. This could potentially cause disruption to users who may have utilized these abilities in the past.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Screen video capture**
6. Ensure **Configuration** is set to **Do not allow sites to prompt the user to share a video stream of their screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Screen video capture**
6. Set **Configuration** to **Do not allow sites to prompt the user to share a video stream of their screen**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ScreenCaptureAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.8.3 (L2) Ensure 'Cookies' is set to 'Session Only' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

When leaving the setting `_RestoreOnStartup_` unset results in the use of `_DefaultCookiesSetting_` for all sites, if it's set. If `_DefaultCookiesSetting_` is not set, the user's personal setting applies.

- **Disabled** (0, user's personal setting applies)
- **Allow all sites to set local data** (1)
- **Do not allow any site to set local data** (2)
- **Keep cookies for the duration of the session** (4)

The recommended state for this setting is: **Enabled** with a value of **Keep cookies for the duration of the session** (4)

NOTE: If the `RestoreOnStartup` setting is set to restore URLs from previous sessions this setting will not be respected and cookies will be stored permanently for those sites. An example of those URLs are SSO or intranet sites.

Rationale:

Permanently stored cookies may be used for malicious intent.

Impact:

If this setting is enabled, cookies will be cleared when the session closes.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cookies**
6. Ensure **Configuration** is set to **Session Only**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cookies**
6. Set **Configuration** to **Session Only**
7. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultCookiesSetting>
2. <https://chromeenterprise.google/policies/#RestoreOnStartup>
3. <https://chromeenterprise.google/policies/#CookiesSessionOnlyForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.8.4 (L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Chrome allows cookies to be set by web page elements that are not from the domain in the user's address bar. Enabling this feature prevents third party cookies from being set.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Blocking third-party cookies can help protect a user's privacy by eliminating a number of website tracking cookies.

Impact:

Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser's address bar.

NOTE: Third Party Cookies and Tracking Protection are required for many business critical websites, including Microsoft 365 web apps (Office 365), Salesforce, and SAP Analytics Cloud. If these, or similar services, are needed by the organization, then this setting can be Disabled.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party cookie blocking**
6. Ensure **Configuration** is set to **Disallow third-party cookies**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party cookie blocking**
6. Set **Configuration** to **Disallow third-party cookies**
7. Select **Save**






Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BlockThirdPartyCookies>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.8.5 (L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls access to the First-Party Sets. First-Party Sets are a way for sites to declare relationships with each other and enable limited cross-site cookie access for specific, user-facing purposes. It can be configured to either:

- Disabled (0): Disable First-Party Sets for all affected users
- Enabled (1): Enable First-Party Sets for all affected users

Rationale:

Setting this policy will not allow sites to declare the relationships that allow them to access the cross-site cookies.

Impact:

This may cause unexpected behavior as a user moves between affiliated sites.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **First-Party Sets**
6. Ensure **Configuration** is set to **Disable First-Party Sets for all affected users**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **First-Party Sets**
6. Set **Configuration** to **Disable First-Party Sets for all affected users**
7. Select **Save**




Default Value:

Enabled

References:

1. <https://chromeenterprise.google/policies/#FirstPartySetsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.8.6 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:

- Disabled (2): Does not allow access to the clipboard site permission by any site
- Enabled (3): Sites ask the user to allow access to the clipboard site permission

If the value for `DefaultClipboardSetting` is not changed from the default, it will behave as if it is enabled. `ClipboardAllowedForUrls` or `ClipboardBlockedForUrls` will override this setting for any site that matches the configured URL patterns.

With the setting disabled, organizations will need to set `ClipboardAllowedForUrls` for any URLs they want to make exempt.

Rationale:

The clipboard stores data, text, and images that are shared between all applications. An organization would disable clipboard access to restrict sites from reading the contents of the clipboard when visiting.

Impact:

Not allowing sites to have access to the clipboard permission can cause issues with formatting or access to needed images on the clipboard.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Devices`
3. Select `Chrome`
4. Select `Settings`
5. Under `User & browser settings`, select `Clipboard`
6. Ensure `Configuration` is set to `Do not allow any site to use the clipboard site permission`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clipboard**
6. Set **Configuration** to **Do not allow any site to use the clipboard site permission**
7. Select **Save**

Default Value:

Allow clipboard permission access

References:






1. <https://chromeenterprise.google/policies/#DefaultClipboardSetting>

Additional Information:

If your organization requires a set of sites permitted to access the clipboard, configure them via this setting in the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Clipboard**
6. Set URLs required by your organization in **Allow these sites to access the clipboard**
7. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.8.7 (L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome offers websites the ability to display desktop notifications. These are push messages which are sent from the website operator through Google infrastructure to Chrome.

- Allow sites to show desktop notifications (1)
- Do not allow any site to show desktop notifications (2)
- Ask every time a site wants to show desktop notifications (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to show desktop notifications (2)

Rationale:

If the website operator decides to send messages unencrypted, Google's servers may process it as plain text. Furthermore, potentially compromised or faked notifications might trick users into clicking on a malicious link.

Impact:

If this setting is enabled and set to Do not allow any site to show desktop notifications, notifications will not be displayed for any sites and the user will not be asked.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Notifications
6. Ensure Configuration is set to Do not allow any site to show desktop notifications

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Notifications**
6. Set **Configuration** to **Do not allow any site to show desktop notifications**
7. Select **Save**

Default Value:

Unset (Same as Enabled, with 'Ask every time a site wants to show desktop notifications')

References:

1. <https://chromeenterprise.google/policies/#DefaultNotificationsSetting>
2. <https://www.google.com/chrome/privacy/whitepaper.html#notifications>
3. <https://medium.com/@BackmaskSWE/push-messages-isnt-secure-enough-69121c683cc6>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.8.8 (L1) *Ensure 'Auto open downloaded files' Is Not Set (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether specified file types are allowed to auto open on download. It also controls specified URLs to allow those specified file types to auto open when they are downloaded from those URLs.

Rationale:

No file types should not be allowed to auto open and the user is required to interact with every downloaded file they wish to open.

Impact:

There is no impact to the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Content**, select **Auto open downloaded files**
6. Ensure **Auto open file types** is not configured
7. Ensure **Auto open URLs** is not configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Content**, select **Auto open downloaded files**
6. Remove all file types from **Auto open file types**
7. Remove all URLs from **Auto open URLs**
8. Select **Save**






Default Value:

Unset (disabled)

References:

1. <https://chromeenterprise.google/policies/#AutoOpenFileTypes>
2. <https://chromeenterprise.google/policies/#AutoOpenAllowedForURLs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.			

2.3.1.8.9 (L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Google Cast is able to connect to all IP Addresses or only private IP Addresses as defined in RFC1918 (IPv4) and RFC4193 (IPv6). Note that if the *EnabledMediaRouter* setting is set to **Disabled** there is no positive or negative effect for this setting.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Allowing Google Cast to connect to public IP addresses could allow media and other potentially sensitive data to be exposed to the public. Disabling this setting will ensure that Google Cast is only able to connect to private (ie: internal) IP addresses.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Ensure **Allow users to Cast from Chrome** is set to **Do not allow users to cast**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Cast**
6. Set **Allow users to Cast from Chrome** to **Do not allow users to cast**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#MediaRouterCastAllowAllIPs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.1.8.10 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Setting controls whether users can add exceptions to allow mixed content for specific sites.

- Do not allow any site to load mixed content (2)
- Allow users to add exceptions to allow mixed content (3)

The recommended state for this setting is: **Enabled** with the value of **Do not allow any site to load mixed content** (2)

NOTE: This policy can be overridden for specific URL patterns using the *InsecureContentAllowedForUrls* and *InsecureContentBlockedForUrls* policies.

Rationale:

Allowing mixed (secure / insecure) content from a site can lead to malicious content being loaded. Mixed content occurs if the initial request is secure over HTTPS, but HTTPS and HTTP content is subsequently loaded to display the web page. HTTPS content is secure. HTTP content is insecure.

Impact:

Users will not be able to mix content.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Control use of insecure content exceptions**
6. Ensure **Configuration** is set to **Do not allow any site to load mixed content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Control use of insecure content exceptions**
6. Set **Configuration** to **Do not allow any site to load mixed content**
7. Select **Save**





Default Value:

Unset (Same as Enabled: Allow users to add exceptions to allow mixed content, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultInsecureContentSetting>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.5 <u>Subscribe to URL-Categorization service</u> Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.			

2.3.1.8.11 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers the feature URL-keyed anonymized data collection. This sends URLs of pages the user visits to Google to optimize its services.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Anonymized data collection shall be disabled, since it is unclear which information exactly is sent to Google. To find out more on what data is collected, read the Google support documentation: [URL-Keyed Pseudonymous Metrics](#).

Impact:

Anonymized data will not be sent to Google to help optimize its services

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enable URL-keyed anonymized data collection**
6. Ensure **Configuration** is set to **Data collection is never active**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enable URL-keyed anonymized data collection**
6. Set **Configuration** to **Data collection is never active**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#UrlKeyedAnonymizedDataCollectionEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

2.3.1.8.12 (L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome has an API which allows the access to nearby Bluetooth devices from the browser with users consent.

- Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API (2)
- Allow sites to ask the user to grant access to a nearby Bluetooth device (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API (2)

Rationale:

A malicious website could exploit a vulnerable Bluetooth device.

Impact:

If this setting is configured, websites can no longer access nearby Bluetooth devices via the API (this includes web cameras, headphones, and other Bluetooth devices) and the user will never be asked.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Web Bluetooth API
6. Ensure Configuration is set to Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Bluetooth API**
6. Set **Configuration** to **Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API**
7. Select **Save**





Default Value:

Unset (Same as Enabled: Allow sites to ask the user to grant access to a nearby Bluetooth device, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultWebBluetoothGuardSetting>
2. https://webbluetoothcg.github.io/web-bluetooth/use-cases.html#security_privacy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	15.9 <u>Disable Wireless Peripheral Access of Devices</u> Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.			

2.3.1.8.13 (L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting will allow specified URLs to access **file://** URLs in the PDF Viewer. By default all domains are blocked from accessing **file://** URLs in the PDF Viewer

Rationale:

Blocking all domains, or a restricted list of domains, from opening a downloaded PDF file blocks the possibility of a malicious file being masked as a PDF. It could also block unknown or malicious code contained within the PDF that would run on the immediate opening within a browser tab.

Impact:

Users will be required to open PDF files manually in the PDF Viewer or in the organization's PDF viewing application.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow local file access to file:// URLs on these sites in the PDF Viewer**
6. Ensure **Allowed URLs** is empty

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow local file access to file:// URLs on these sites in the PDF Viewer**
6. Remove all URLs from **Allowed URLs**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PdfLocalFileAccessAllowedForDomainS>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u> Train workforce members to be able to recognize a potential incident and be able to report such an incident.			
v7	3.3 <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.			

2.3.1.8.14 (L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting will block any site from accessing the storage session from any other site. This will block third party trackers that are embedded on multiple sites from tracking a user across the sites they visit. Blocking third party access to the user agent will not allow sites to infer data about the user from the data from another site.

It can be configured to either:

- Enabled (1): Allow third-party storage partitioning to be enabled.
- Disabled (2): Block third-party storage partitioning from being enabled.

Rationale:

Setting this requires that user agent state needs to be keyed by more than a single origin or site. It can also defend against timing attacks on web privacy.

Impact:

Enforcing this may cause users to experience issues with sites they regularly visit that already grant access to third-parties.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Ensure **Configuration** is set to **Block third-party storage partitioning from being enabled**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Third-party storage partitioning**
6. Set **Configuration** to **Block third-party storage partitioning from being enabled**
7. Select **Save**

Default Value:

Not Configured

References:

1. <https://chromeenterprise.google/policies/#DefaultThirdPartyStoragePartitioningSetting>
2. <https://privacycg.github.io/storage-partitioning/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u> Train workforce members to be able to recognize a potential incident and be able to report such an incident.	●	●	●
v7	3.3 <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●

2.3.1.9 User experience

2.3.1.9.1 (L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers to download files automatically to the default download directory without prompting.

If this setting is enabled, users are always asked where to save each file before downloading.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Users shall be prevented from the drive-by-downloads threat.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download location prompt**
6. Ensure **Configuration** is set to **Ask the user where to save the file before downloading**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download location prompt**
6. Set **Configuration** to **Ask the user where to save the file before downloading**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PromptForDownloadLocation>
2. <https://www.ghacks.net/2017/05/18/you-should-disable-automatic-downloads-in-chrome-right-now/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.9.2 (L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can use Google web service to help resolve spelling errors.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Information typed in may be leaked to Google's spellcheck web service.

Impact:

After disabling this feature, Chrome no longer sends the entire contents of text fields to Google as you type them. Spell checking can still be performed using a downloaded dictionary. This setting only controls the usage of the online service.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Spell check service**
6. Ensure **Configuration** is set to **Disable the spell checking web service**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Spell check service**
6. Set **Configuration** to **Disable the spell checking web service**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SpellCheckServiceEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.3 (L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting enables Google translation services on Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Content of internal web pages may be leaked to Google's translation service.

Impact:

After disabling this feature, the contents of a web page are no longer sent to Google for translation.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google Translate**
6. Ensure **Configuration** is set to **Never offer translation**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Google Translate**
6. Set **Configuration** to **Never offer translation**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#TranslateEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.4 (L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers to show suggestions for the page you were trying to reach when it is unable to connect to a web address such as 'Page Not Found'.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Using navigation suggestions may leak information about the web site intended to be visited.

Impact:

If this setting is disabled, Chrome will no longer use a web service to help resolve navigation errors.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Alternate error pages**
6. Ensure **Configuration** is set to **Never use alternate error pages**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Alternate error pages**
6. Set **Configuration** to **Never use alternate error pages**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AlternateErrorPagesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.5 (L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Chrome allows users to auto-complete web forms with saved information such as address or phone number. Disabling this feature will prompt a user to enter all information manually.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If an attacker gains access to a user's machine where the user has stored address AutoFill data, information could be harvested.

Impact:

If this setting is disabled, AutoFill will be inaccessible to users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Address form Autofill**
6. Ensure **Configuration** is set to **Never Autofill address forms**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Address form Autofill**
6. Set **Configuration** to **Never Autofill address forms**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AutofillAddressEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.6 (L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Chrome allows users to auto-complete web forms with saved credit card information. Disabling this feature will prompt a user to enter all information manually.

The recommended state for this setting is: **Disabled** (0)

Rationale:

If an attacker gains access to a user's machine where the user has stored credit card AutoFill data, information could be harvested.

Impact:

If this setting is disabled, credit card AutoFill will be inaccessible to users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Credit card form Autofill**
6. Ensure **Configuration** is set to **Never Autofill credit card forms**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Credit card form Autofill**
6. Set **Configuration** to **Never Autofill credit card forms**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AutofillCreditCardEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.7 (L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows you to set whether a website can check to see if the user has payment methods saved.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Saving payment information in Google Chrome could lead to sensitive data being leaked and used for non-legitimate purposes.

Impact:

Websites will be unable to query whether payment information within Google Chrome is available.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Payment methods**
6. Ensure **Configuration** is set to **Always tell websites that no payment methods are saved**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Payment methods**
6. Set **Configuration** to **Always tell websites that no payment methods are saved**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#PaymentMethodQueryEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.8 (L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome comes with the network prediction feature which provides DNS prefetching, TCP and SSL preconnection, and prerendering of web pages.

- Predict network actions on any network connection (0) or (1)
- Do not predict network actions on any network connection (2)

The recommended state for this setting is: Enabled with a value of Do not predict network actions on any network connection (2)

Rationale:

Opening connections to resources that may not be used could allow unneeded connections, increasing the attack surface, and in some cases could lead to opening connections to resources which the user did not intend to utilize.

Impact:

Users will not be presented with web page predictions.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Network prediction
6. Ensure Configuration is set to Do not predict network actions

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Network prediction**
6. Set **Configuration** to **Do not predict network actions**
7. Select **Save**

Default Value:

Unset (Same as Enabled with a value of Predict network actions on any network connection)

References:

1. <https://chromeenterprise.google/policies/#NetworkPredictionOptions>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.1.9.9 (L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls whether a user may utilize guest profiles in Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

In a guest profile, the browser doesn't import browsing data from existing profiles, and it deletes browsing data when all guest profiles are closed.

Deleting browser data will delete information that may be important for a computer investigation, and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Users will not be able to initiate Guest mode for Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser guest mode**
6. Ensure **Configuration** is set to **Prevent guest browser logins**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Browser guest mode**
6. Set **Configuration** to **Prevent guest browser logins**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#BrowserGuestModeEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.10 (L2) Ensure 'Native Messaging blocked hosts' is set to '*' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Allows you to specify which native messaging hosts should not be loaded.

Disabled (0): Google Chrome will load all installed native messaging hosts.

The recommended state for this setting is: **Enabled** with a value of *

NOTE: This needs to be handled carefully. If an extension is enabled, yet can't communicate with its backend code, it could behave in strange ways which results in helpdesk tickets + support load.

Rationale:

For consistency with Plugin and Extension policies, native messaging should be blocklisted by default, requiring explicit administrative approval of applications for allowlisting. An example of an application that uses native messaging is the 1Password password manager.

Impact:

A blocklist value of '*' means all native messaging hosts are blocklisted unless they are explicitly listed in the allowlist.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Native Messaging blocked hosts**
6. Ensure **Prohibited Native Messaging hosts** is set to *

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Native Messaging blocked hosts**
6. Set **Prohibited Native Messaging hosts** to *
7. Select **Save**





Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#NativeMessagingBlocklist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.3.1.9.11 (L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether users are able to utilize the Chrome feedback feature to send feedback, suggestions, and surveys to Google, as well as issue reports.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Data should not be shared with third-party vendors in an enterprise managed environment.

Impact:

Users will not be able to send feedback to Google.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow user feedback**
6. Ensure **Configuration** is set to **Do not allow user feedback**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow user feedback**
6. Set **Configuration** to **Do not allow user feedback**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#UserFeedbackAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.9.12 (L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting allows access to local files by allowing file selection dialogs in Google Chrome.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Allowing users to import favorites, upload files, and save links could pose potential security risks by allowing data to be uploaded to external sites or by downloading malicious files. By not allowing the file selection dialog, the end-user will not be prompted for uploads/downloads, preventing data exfiltration and possible system infection by malware.

Impact:

If you disable this setting, users will no longer be prompted when performing actions which would trigger a file selection dialog. Instead, the file selection dialog box assumes the user clicked "Cancel". Being as this is not the default behavior, impact to the user will be noticeable, and the user will not be able to upload and download files.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File selection dialogs**
6. Ensure **Configuration** is set to **Block file selection dialogs**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **File selection dialogs**
6. Set **Configuration** to **Block file selection dialogs**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AllowFileSelectionDialogs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.5 Integrate Software and Hardware Asset Inventories The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●

2.3.1.10 Connected devices

The **Connected devices** sub-section deals with the interaction between Android devices with computers running the Chrome browser or running ChromeOS. With the requirement of additional devices, we are not giving any guidance on using **Connected devices**. We are recommending your organization goes through this section and makes determinations on how these should be configured.

2.3.1.11 Omnibox Search Provider

Omnibox search provider settings are configuration options in the Google admin console for managing search options in Chrome browsers within an organization.

Administrators can control how user's interact with the omnibox in the Chrome browser on managed devices, including search suggestions, side panel configurations, history searches, and even what default search provider the browser will use.

2.3.1.11.1 (L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome offers suggestions in Google Chrome's omnibox while a user is typing.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Using search suggestions may leak information as soon as it is typed/pasted into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Impact:

The user has to send the search request actively by using the search button or hitting "Enter".

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Search suggest**
6. Ensure **Configuration** is set to **Never allow users to use Search Suggest**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Search suggest**
6. Set **Configuration** to **Never allow users to use Search Suggest**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SearchSuggestEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.11.2 (L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the Google Search Side Panel. It can be configured to either:

- Disabled (0): **Disable Google Search Side Panel on all web pages**
- Enabled (1): **Enable Google Search Side Panel on all web pages**

Rationale:

Setting this policy will not allow the Google Search Side Panel on any webpages.

Impact:

This should have no user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Side Panel search**
6. Ensure **Configuration** is set to **Disable Side Panel search on all web pages**

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Side Panel search**
6. Set **Configuration** to **Disable Side Panel search on all web pages**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#GoogleSearchSidePanelEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.12 Hardware

2.3.1.12.1 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome has an API which allows access to connected USB devices from the browser

- Do not allow any site to request access to USB devices via the WebUSB API (2)
- Allow sites to ask the user to grant access to a connected USB device (3)

The recommended state for this setting is: Enabled with a value of Do not allow any site to request access to USB devices via the WebUSB API (2)

Rationale:

WebUSB is opening the doors for sophisticated phishing attacks that could bypass hardware-based two-factor authentication devices (e.g. Yubikey devices).

Impact:

If this setting is configured, websites can no longer access connected USB devices via the API (this includes web cameras, headphones, and other USB devices) which could also prevent some two factor authentication (2FA) USB devices from working properly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select WebUSB API
6. Ensure Configuration is set to Do not allow any site to request access to USB devices via the WebUSB API

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **WebUSB API**
6. Set **Configuration** to **Do not allow any site to request access to USB devices via the WebUSB API**
7. Select **Save**





Default Value:

Unset (Same as Enabled: Allow sites to ask the user to grant access to a connected USB device, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultWebUsbGuardSetting>
2. <https://www.wired.com/story/chrome-yubikey-phishing-webusb/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

2.3.1.12.2 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting allows administrators to set whether the end-user is prompted for access to audio capture devices.

- **Disabled** (0): Turns off prompts and audio capture will only work for URLs configured in the *AudioCaptureAllowedUrls* list.
- **Enabled** (1): With the exception of URLs set in the *AudioCaptureAllowedUrls* list, users get prompted for audio capture access.

NOTE: The setting affects all audio input (not just the built-in microphone).

The recommended state for this setting is: **Disabled**

Rationale:

The end-user having the ability to allow or deny audio capture for websites in Google Chrome could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing audio capture, it removes the end-user's discretion, leaving it up to the organization which sites are allowed to use this ability.

Impact:

If you disable this setting, users will not be prompted for audio devices when using websites which may need this access, such as a web-based conferencing system. If there are sites to which access will be allowed, configuration of the *AudioCaptureAllowedUrls* setting will be necessary.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio input (microphone)**
6. Ensure **Configuration** is set to **Disable audio input**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Audio input (microphone)**
6. Set **Configuration** to **Disable audio input**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AudioCaptureAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.12.3 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting allows administrators to set whether the end-user is prompted for access to video capture devices.

- **Disabled** (0): Turns off prompts and video capture will only work for URLs configured in the *VideoCaptureAllowedUrls* list.
- **Enabled** (1): With the exception of URLs set in the *VideoCaptureAllowedUrls* list, users get prompted for video capture access.

NOTE: The setting affects all video input (not just the built-in camera).

The recommended state for this setting is: **Disabled** (0)

Rationale:

The end-user having the ability to allow or deny video capture for websites in Google Chrome could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing video capture, it removes the end-user's discretion, leaving it up to the organization which sites are allowed to use this ability.

Impact:

If you disable this setting, users will not be prompted for video devices when using websites which may need this access, such as a web-based conferencing system. If there are sites to which access will be allowed, configuration of the *VideoCaptureAllowedUrls* setting will be necessary.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Video input (camera)**
6. Ensure **Configuration** is set to **Disable camera input for websites and apps**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Video input (camera)**
6. Set **Configuration** to **Disable camera input for websites and apps**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#VideoCaptureAllowed>
2. <https://chromeenterprise.google/policies/#VideoCaptureAllowedUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.12.4 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls website access and use of the system serial port.

- Do not allow any site to request access to serial ports via the Serial API (2)
- Allow sites to ask the user to grant access to a serial port (3)

The recommended state for this setting is: Do not allow any site to request access to serial ports via the Serial API (2)

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SerialAllowAllPortsForUrls*, *SerialAskForUrls* and *SerialBlockedForUrls* settings. For example, *SerialAllowAllPortsForUrls* can be used to allow serial port access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system serial ports may prevent malicious sites from using these ports and accessing the devices attached.

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Serial API**
6. Ensure **Configuration** is set to **Do not allow any site to request access to serial ports via the Web Serial API**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Web Serial API**
6. Set **Configuration** to **Do not allow any site to request access to serial ports via the Web Serial API**
7. Select **Save**

Default Value:

Unset (Same as Enabled with Allow sites to ask the user to grant access to a serial port, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSerialGuardSetting>
2. <https://chromeenterprise.google/policies/#SerialAskForUrls>
3. <https://chromeenterprise.google/policies/#SerialBlockedForUrls>
4. <https://chromeenterprise.google/policies/#SerialAllowAllPortsForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.1.12.5 (L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The privacy screen for ChromeOS is a feature that activates when the user walks away from the Chromebook. If activated, the screen will dim after 10 seconds. It can also keep the screen awake while the user is in front of the Chromebook even if they are not interacting with the device.

This policy requires a built in webcam and for ChromeOS devices with an integrated electronic privacy screen.

Rationale:

Setting the operating system to automatically dim and lock the screen when the user moves away from the device protects potentially sensitive data that may reside on their machine.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Hardware**, select **Privacy screen**
6. Ensure **Privacy screen** is set to **Always enable the privacy screen**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Hardware**, select **Privacy screen**
6. Set **Privacy screen** to **Always enable the privacy screen**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PrivacyScreenEnabled>
2. <https://support.google.com/chromebook/answer/12212810?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u> Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			
v7	16.1 <u>Maintain an Inventory of Authentication Systems</u> Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.			

2.3.1.12.6 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls website access and use of system sensors such as motion and light.

- Allow sites to access sensors (1)
- Do not allow any site to access sensors (2)

The recommended state for this setting is: Do not allow any site to access sensors (2)

The recommended state for this setting is: Enabled with a value of Do not allow any site to access sensors

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SensorsAllowedForUrls* and *SensorsBlockedForUrls* settings. For example, *SensorsAllowedForUrls* can be used to allow sensor access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system sensors may prevent malicious sites from using these sensors for user profiling (OpSec).

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Under User & browser settings, select Sensors
6. Ensure Configuration is set to Do not allow any site to access sensors

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Sensors**
6. Set **Configuration** to **Do not allow any site to access sensors**
7. Select **Save**





Default Value:

Unset (Same as Enabled with a value of Allow sites to access sensors, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSensorsSetting>
2. <https://chromeenterprise.google/policies/#SensorsAllowedForUrls>
3. <https://chromeenterprise.google/policies/#SensorsBlockedForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.1.12.7 (L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows extensions installed by enterprise policies to be allowed to use the Enterprise Hardware Platform API.

The recommended state for this setting is: **Disabled** (0)

Rationale:

It is recommended that this setting is disabled unless otherwise directed by Enterprise policies.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enterprise Hardware Platform API**
6. Ensure **Configuration** is set to **Do not allow managed extensions to use the Enterprise Hardware Platform API**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Enterprise Hardware Platform API**
6. Set **Configuration** to **Do not allow managed extensions to use the Enterprise Hardware Platform API**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#EnterpriseHardwarePlatformAPIEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.1.13 User verification

2.3.1.13.1 (L2) Ensure 'Verified Mode' Is Set to 'Require verified mode boot for Verified Access' (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Verified Access ensures that a device connecting to your network has been unmodified and is policy-compliant. Verified Access serves as an access point for a network service (such as a VPN gateway, a sensitive server, an enterprise Certificate Authority [CA], or an enterprise Wi-Fi access point) to get a hardware-backed cryptographic guarantee of the identity of the device and user that's trying to access it.

Verified Access uses the Trusted Platform Module (TPM) - present in every Chrome OS device - to enable enterprise network services to cryptographically confirm the identity and status of secure mode and enterprise policy using a Google server-side Application Programming Interface (API).

Rationale:

The Chrome Verified Access API allows network services, such as VPNs, intranet pages, and so on to cryptographically verify that their clients are genuine and conform to corporate policy. Most large enterprises have the requirement to allow only enterprise-managed devices onto their WPA2 EAP-TLS networks, higher-tier access in VPNs, and mutual-TLS intranet pages.

Impact:

This would impact a user that is required to use a development branch of ChromeOS.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User verification**, select **Verified Mode**
6. Ensure **Verified Mode boot check** is set to greater than or equal to **Do not show the display password button on the login and lock screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User verification**, select **Verified Mode**
6. Set **Verified Mode boot check** to **Verified Mode**
7. Select **Save**

References:

1. <https://support.google.com/chrome/a/answer/7156268>

Additional Information:

To properly configure Verified Mode, your organization will need to create both a Chrome extension and a network service endpoint. To set up both the extension and the network service endpoint, follow the instructions in the [Chrome Verified Access Developer's Guide](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

2.3.1.14 Browser Reporting

2.3.1.14.1 (L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls the upload of information from the operation of the browser to your organization's Google Admin console.

By default, this policy is disabled and there is no data collected. When enabled, the data is collected and uploaded to the Google Admin console.

Note: For Chrome browser, this policy requires your organization to use Chrome Browser Cloud Management (CBCM). CBCM is not required for ChromeOS.

Rationale:

Enabling logging will give your organization a detailed view of ChromeOS, the Chrome browser, and the extensions in use.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Browser reporting**, select **Managed browser reporting**
6. Ensure **Browser reporting** is set to **Enable managed browser cloud reporting**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Browser reporting**, select **Managed browser reporting**
6. Set **Browser reporting** to **Enable managed browser cloud reporting**
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#CloudReportingEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

2.3.1.14.2 (L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls the frequency of uploads of the Chrome status reports to your organization's Google Admin console. This policy includes the reports when setting **Managed browser reporting** to **Enable managed browser cloud reporting**.

When unset, this policy defaults to uploading status reports every 24 hours. If set to another time amount, the policy will upload successive status reports as defined by the policy.

Rationale:

The frequency of uploads should match your organization's requirements but should not exceed 24 hours. This allows faster response to any anomalies.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Browser reporting**, select **Managed browser reporting upload frequency**
6. Ensure **Managed browser reporting upload frequency** is set **≤24**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Browser reporting**, select **Managed browser reporting upload frequency**
6. Set **Managed browser reporting upload frequency** to ≤ 24
7. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#CloudReportingUploadFrequency>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

2.3.1.15 Chrome Safe Browsing

2.3.1.15.1 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Google Chrome's Safe Browsing feature is enabled and the mode in which it operates. If you set this setting as mandatory, users cannot change or override the Safe Browsing setting in Google Chrome.

If this setting is left unset, Safe Browsing will operate in Standard Protection mode. Users, however, can change this setting.

- **No Protection** (0): Safe Browsing is never active.
- **Standard Protection** (1): Safe Browsing is active in the standard mode.
- **Enhanced Protection** (2): Safe Browsing is active in the enhanced mode. This mode provides better security, but requires sharing more browsing information with Google.

The recommended state for this setting is: **Safe Browsing is active in the standard mode.** (1) or higher

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or from downloading dangerous files.

NOTE: Google recommends using Enhanced Safe Browsing Mode (2). Turning on Enhanced Safe Browsing will substantially increase protection from dangerous websites and downloads, but will share more data with Google.

For more details, please refer to the items in the References section below.

Impact:

None - This is the default behavior (Standard Protection).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing protection**
6. Ensure **Safe Browsing Protection Level** is set to **Safe Browsing is active in the standard mode**
7. Ensure **Safe Browsing standard protection real time proxied checks** is set to **Allow real time proxied checks**
8. Ensure **User override** is set to **Do not allow users to override this setting**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing protection**
6. Set **Safe Browsing Protection Level** to **Safe Browsing is active in the standard mode**
7. Set **Safe Browsing standard protection real time proxied checks** to **Allow real time proxied checks**
8. Set **User override** to **Do not allow users to override this setting**
9. Select **Save**





Default Value:

Unset (Same as Standard Protection, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingProtectionLevel>
2. <https://security.googleblog.com/2020/05/enhanced-safe-browsing-protection-now.html>
3. <https://security.googleblog.com/2021/06/new-protections-for-enhanced-safe.html>
4. https://developers.google.com/safe-browsing?_ga=2.65351149.274800631.1631808382-2031399475.1630502681

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.15.2 (L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The setting determines the functionality of Safe Browsing.

- **Disabled** (0): Safe Browsing protection applies to all resources
- **Enabled** (1), with a list of 1 or more sites: Means Safe Browsing will trust the domains you designate. It won't check them for dangerous resources such as phishing, malware, or unwanted software.

The recommended state for this setting is: **Disabled** (0)

NOTE: Safe Browsing's download protection service won't check downloads hosted on these domains, and its password protection service won't check for password reuse.

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites, or from downloading dangerous files.

Impact:

None - This is the default behavior.

NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing allowed domains**
6. Ensure **Allow Domains** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing allowed domains**
6. Remove any URLs from **Allowed Domains**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingAllowlistDomains>
2. <https://safebrowsing.google.com/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.15.3 (L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can be adjusted to allow downloads without Safe Browsing checks when the requested file is from a trusted source. Trusted sources can be defined using recommendation 'Configure the list of domains on which Safe Browsing will not trigger warnings'.

The recommended state for this setting is: **Disabled** (0)

NOTE: On Microsoft Windows, this functionality is only available on instances that are joined to a Microsoft Active Directory domain, running on Windows 10 Pro, or enrolled in Chrome Browser Cloud Management.

Rationale:

Information requested from trusted sources shall not be sent to Google's safe browsing servers.

Impact:

If this setting is disabled, files downloaded from intranet resources will not be checked by Google Services.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing for trusted sources**
6. Ensure **Configuration** is set to **Perform Safe Browsing checks on all downloaded files**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Safe Browsing for trusted sources**
6. Set **Configuration** to **Perform Safe Browsing checks on all downloaded files**
7. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingForTrustedSourcesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 Use DNS Filtering Services Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.1.15.4 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can block certain types of downloads, and won't let users bypass the security warnings, depending on the classification of Safe Browsing.

- No special restrictions. Default. (0, Disabled) (Default)
- Block malicious downloads and dangerous file types. (1)
- Block malicious downloads, uncommon or unwanted downloads, and dangerous file types. (2)
- Block all downloads. (3)
- Block malicious downloads. Recommended. (4)

The recommended state for this setting is: **Enabled** with a value of **Block malicious downloads. Recommended.** (4)

NOTE: These restrictions apply to downloads triggered from webpage content, as well as the "Download link..." menu option. They don't apply to the download of the currently displayed page or to saving as PDF from the printing options.

Rationale:

Users shall be prevented from downloading malicious file types and shall not be able to bypass security warnings.

Impact:

If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings. These are downloads that have been identified as risky or from a risky source by the [Google Safe Browsing Global intelligence engine](#).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download restrictions**
6. Ensure **Configuration** is set to **Block malicious downloads**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Download restrictions**
6. Set **Configuration** to **Block malicious downloads**
7. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DownloadRestrictions>
2. <https://developers.google.com/safe-browsing>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.3.1.15.5 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google provides the Safe Browsing service. It shows a warning page when users navigate to sites that are flagged as potentially malicious.

Disabled (0): Users can choose to proceed to the flagged site after the warning appears.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Malicious web pages are widely spread on the internet and pose the most significant threat to the user today. Users shall be prevented from navigating to potentially malicious web content.

Impact:

Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. In some cases legitimate sites could be blocked and users would be prevented from accessing.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disable bypassing Safe Browsing warnings**
6. Ensure **Configuration** is set to **Do not allow user to bypass Safe Browsing warning**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Disable bypassing Safe Browsing warnings**
6. Set **Configuration** to **Do not allow user to bypass Safe Browsing warning**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DisableSafeBrowsingProceedAnyway>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.15.6 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome can use the Google Safe Search API to classify URLs as pornographic or not.

The recommended state for this setting is: **Filter top level sites (but not embedded iframes) for adult content**

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are more prone to malicious content including spyware, adware, and viruses.

Impact:

Users' search results will be filtered and content such as adult text, videos, and images will not be shown.

NOTE: Using Google's Safe Search API may leak information which is typed/pasted by mistake into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSites URL filter**
6. Ensure **Configuration** is set to **Filter top level sites (but not embedded iframes) for adult content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **SafeSites URL filter**
6. Set **Configuration** to **Filter top level sites (but not embedded iframes)** for adult content
7. Select **Save**





Default Value:

Unset (Same as Enabled with "Do not filter sites for adult content", but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeSitesFilterBehavior>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.15.7 (L1) *Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting prevents the display of lookalike URL warnings on the sites listed. These warnings are typically shown on sites that Google Chrome believes might be trying to spoof another site with which the user is familiar.

- **Disabled** (0) or set to an empty list: Warnings may appear on any site the user visits.
- **Enabled** (1) and set to one or more domains: No lookalike warnings pages will be shown when the user visits pages on that domain.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Look-alike domains are intentionally misleading to give users the false impression that they're interacting with trusted brands, leading to significant reputation damage, financial losses, and data compromise for established enterprises.

In addition, this technique is commonly used to host phishing sites, and often leads to account takeover attacks. Users are prompted to enter their credentials on a fake website, and scammers take control of their online accounts with little effort to engage in fraudulent activity.

Impact:

None - This is the default behavior.

NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Suppress lookalike domain warnings on domains**
6. Ensure **Allowlisted Domains** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Suppress lookalike domain warnings on domains**
6. Remove all URLs from **Allowlisted Domains**
7. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#LookalikeWarningAllowlistDomains>
2. <https://safebrowsing.google.com/>
3. <https://bugs.chromium.org/p/chromium/issues/entry?template=Safety+Tips+Appeals>
4. <https://krebsonsecurity.com/2018/03/look-alike-domains-and-visual-confusion/>
5. <https://www.phishlabs.com/blog/the-anatomy-of-a-look-alike-domain-attack/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.15.8 (L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **Abusive Experience Intervention** is a proactive security measure that uses automated detection and a tiered enforcement system to protect users from deceptive online practices that can lead to phishing, malware, and a degraded browsing experience.

Rationale:

Abusive Experience Intervention provides a strong security rationale rooted in a proactive, user-centric approach to online safety. Rather than just reacting to known threats like malware, it focuses on preventing the user from ever being put in a position to be exploited in the first place.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Abusive Experience Intervention**
6. Ensure **Configuration** is set to **Prevent sites with abusive experiences from opening new windows or tabs**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Abusive Experience Intervention**
6. Set **Configuration** to **Prevent sites with abusive experiences from opening new windows or tabs**
7. Select **Save**





Default Value:

Unset (same as enabled)

References:

1. <https://chromeenterprise.google/policies/#AbusiveExperienceInterventionEnforce>
2. <https://support.google.com/webtools/answer/7539006?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.16 Generative AI

Generative AI settings are configuration options in the Google admin console for managing various aspects of how users interact with AI features in the Chrome browser within an organization. This includes features like text generation, search enhancements, and comparison tools, enabling customization of the browsing experience to meet specific organizational needs and security policies.

The security recommendations provided are based on the assumption that an organization utilizes AI-powered products. A trust relationship with the technology vendor is essential, as sensitive data may be stored on their servers, similar to email and cloud storage. However, some features of the AI model also require the level of trust between customers of the AI model. If your data is used to train the AI model, then the other customers of the AI model can receive guidance that could be based on your organization's data. Enabling any AI feature(s) should be driven by organizational requirements.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended settings or disabling the feature(s) based on organizational needs.

Note: Ensure proprietary data is not used for AI model training to prevent data leaks.

2.3.1.16.1 Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **Generative AI policy defaults** sets the default options for all policies in the **Generative AI** feature set if those setting are unset. This policy will be overridden for any settings that are set individually.

The **Generative AI policy defaults** can only be set in the Google Admin Console and cannot be set locally.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Setting a default baseline for all the settings in the **Generative AI** section and will also encompass any new settings as they are added to the Google Admin Console. To find what features are currently available and set through the **Generative AI policy defaults** you can visit the [Chrome—Generative AI features and policies](#)

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Generative AI policy defaults**
6. Ensure **Configuration** is set to **Allow GenAI features without improving AI models**

Note:* For compliance, adherence to security recommendations is also achieved by ensuring **Configuration** is set to **Do not allow GenAI features**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Generative AI policy defaults**
6. Set **Configuration** to **Allow GenAI features without improving AI models**
7. Select **Save**

*Note:** For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow GenAI features**.

Default Value:

Allow GenAI features without improving AI models is the default for Enterprise users managed by Google Admin console and for Education accounts managed by Google Workspace.

References:

1. <https://chromeenterprise.google/policies/#GenAiDefaultSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.16.2 Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Help me write is an AI-based assistant that helps a user write web content, and is based on prompts entered by the user and the contents of the web page.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **Help me write** feature to improve the AI model's content can stop possible leakage of your organization's propriety information if it is used in the prompts to create the content.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me write**
6. Ensure **Configuration** is set to **Allow help me write without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me write**
6. Set **Configuration** to **Allow help me write without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#HelpMeWriteSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.16.3 Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

DevTools AI features is an AI-based assistant that provides additional debugging information. It requires the sending of error messages, stack traces, code snippets, network requests, and/or any other data collected for debugging purposes to Google to train the generative AI model. That data could include prompts, inputs, outputs, source materials, and written feedback, depending on the feature, and may also be reviewed by humans to improve AI models.

Note: Response body or authentication and cookie headers in network requests are not included in the data sent to the server.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **DevTools AI features** feature to improve the AI model's content can stop possible leakage of your organization's propriety information of internal webs in the collected data.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **DevTools AI features**
6. Ensure **Configuration** is set to **Allow DevTools Generative AI Features without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow DevTools Generative AI Features**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **DevTools AI features**
6. Set **Configuration** to **Allow DevTools Generative AI Features without improving AI models** (or Use the value specified in the **Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow DevTools Generative AI Features**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#DevToolsGenAiSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.16.4 Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

History search settings is an AI-based assistant that helps search their browsing history and can receive generated answers based on page contents in addition to just page title and URL.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **History search settings** feature to improve the AI model's content can stop possible leakage of both your organization's propriety information through visited sites as well as any PPI from sites visited.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **History search settings**
6. Ensure **Configuration** is set to **Allow AI history search without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow AI history search**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **History search settings**
6. Set **Configuration** to **Allow AI history search without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow AI history search**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#HistorySearchSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.16.5 Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Tab compare is an AI-based tool for comparing product information across a user's tabs. This feature can be offered to the user when multiple tabs with products in a similar category are open.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **Tab compare** feature to improve the AI model's content can stop possible leakage of your organization's propriety information, or PII, if it is used.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Tab compare**
6. Ensure **Configuration** is set to **Allow tab compare without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow tab compare**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Tab compare**
6. Set **Configuration** to **Allow tab compare without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow tab compare**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. <https://chromeenterprise.google/policies/#TabCompareSettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 <u>Classify Service Providers</u> Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.16.6 Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Help me read is an AI-based assistant that helps a user read web content, and is based on prompts entered by the user and the contents of the web page.

Note: For compliance, adherence to security recommendations is achieved by either implementing the recommended setting or disabling the feature(s) based on organizational needs.

Rationale:

Not allowing the **Help me read** feature to improve the AI model's content can stop possible leakage of your organization's propriety information if used by the AI.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me read**
6. Ensure **Configuration** is set to **Allow help me read without improving AI models** (or **Use the value specified in the Generative AI policy defaults setting**)

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **Generative AI**, select **Help me read**
6. Set **Configuration** to **Allow help me read without improving AI models**
(or **Use the value specified in the Generative AI policy defaults setting**)
7. Select **Save**

Note: For compliance, adherence to security recommendations is also achieved by setting **Configuration** to **Do not allow help me write**.

Default Value:

Unset (will follow the policy set in **GenAiDefaultSettings**)

References:

1. https://admin.google.com/u/1/ac/chrome/settings/user/details/help_me_read_settings_setting_group?ac_ouid=03ph8a2z4j7oqvq&rapt=AEjHL4NFISArXbekf4eV1jk0pYWliEuKs3T-mhnlWY6a13UObuTB6NziLuytTb0Qhkyfcz6x1p2T5ifA0xqwN1WzsdbhUc4wzJO2lOWboSs5-6gRIXP56CA

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.1.17 Chrome updates

2.3.1.17.1 (L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome's Component Updater updates several components of Google Chrome on a regular basis (applies only to Chrome browser components).

The recommended state for this setting is: **Enabled** (1)

NOTE: Updates to any component that does not contain executable code, does not significantly alter the behavior of the browser, or is critical for its security will not be disabled (E.g. certificate revocation lists and Safe Browsing data is updated regardless of this setting). FYI **chrome://components** lists all components, but not if they are affected by this setting.

NOTE: Google provided the following list of **some of the components** controlled by this setting:

- Recovery component
- Pnacl
- Floc
- Optimization hints
- SSL error assistant
- CRL set
- Origin trials
- SW reporter
- PKI metadata

Rationale:

Google Chrome Updater shall be used to keep the components bundled to Chrome up to date.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Component updates**
6. Ensure **Configuration** is set to **Enable updates for all components**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Component updates**
6. Set **Configuration** to **Enable updates for all components**
7. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)







References:

1. <https://chromeenterprise.google/policies/#ComponentUpdatesEnabled>

Additional Information:

To check the current components versions, navigate to <chrome://components>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

2.3.1.17.2 (L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome allows administrators to set the time period, in milliseconds, over which users are notified that it must be relaunched to apply a pending update.

If not set, or **Disabled**, the default period of 604800000 milliseconds (7 days) is used.

The recommended state for this setting is: **Enabled** with value **86400000** (1 day)

Rationale:

This setting is a notification for the end-user informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization, it is pertinent that said update takes effect as soon as possible. Enabling this notification will ensure users restart the browser in a timely fashion.

Impact:

After this time period, the user will be repeatedly informed of the need for an update until a Browser restart is completed.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Ensure **Time Period (hours)** is set to a value **≤168**
7. Ensure **Initial quiet period (hours)** is set to a value **<** the value of **Time Period (hours)**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Set **Time Period (hours)** to a value ≤ 168
7. Set **Initial quiet period (hours)** to a value $<$ the value of **Time Period (hours)**
8. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RelaunchNotificationPeriod>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

2.3.1.17.3 (L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can notify users that it must be restarted to apply a pending update. This setting controls how users are notified to relaunch Chrome browser or restart their ChromeOS device to get the latest update.

The control can be set to one of three options:

- No relaunch notification: Activates a minimal default level of notifications. Chrome browser indicates to users that a relaunch is needed via subtle changes to its menu. In ChromeOS, a notification in the system tray prompts the user to relaunch.
- Show notification recommending relaunch: Users see a recurring message that they should relaunch Chrome browser or restart their ChromeOS device. Users can close the notification and keep using the old version of Chrome browser or ChromeOS until they choose to relaunch Chrome browser or restart their ChromeOS device.
- Force relaunch after a period: Users can close the notification but will see a recurring message that they need to relaunch Chrome browser or restart their ChromeOS device within a certain amount of time.

The recommended state for this setting is: **Enabled** with a value of **Show a recurring prompt to the user indicating that a relaunch is required** (2)

Rationale:

The end-user will receive a notification informing them that an update has been applied and that the browser must be restarted in order for the update to be completed. Once updates have been pushed by the organization it is pertinent that the update is applied as soon as possible. Enabling this notification will ensure that users restart their browser in a timely fashion.

Impact:

A recurring warning will be shown to the user indicating that a browser relaunch will be forced once the notification period passes. The user's session is restored after the relaunch of Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Ensure **Configuration** is set to **Show notification recommending relaunch**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Relaunch notification**
6. Set **Configuration** to **Show notification recommending relaunch**
7. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RelaunchNotification>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

2.3.1.18 Chrome variations

2.3.1.18.1 (L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Configuring this setting allows specifying which variations are allowed to be applied in Google Chrome. Variations provide a means for Google to offer modifications to Google Chrome without shipping a new version of the browser by selectively enabling or disabling already existing features.

- **Enable all variations**: Allows all variations to be applied to the browser (Default value).
- **Enable variations concerning critical fixes only**: Allows only variations considered critical security or stability fixes to be applied to Google Chrome.
- **Disable all variations**: Prevent all variations from being applied to the browser. Please note that this mode can potentially prevent the Google Chrome developers from providing critical security fixes in a timely manner and is thus not recommended.

The recommended state for this setting is: **Enable all variations** (0)

NOTE: Google strongly believes there is no added security benefit for turning this to critical fixes, as leaving it on increases the stability of the browser. Disabling variations can also prevent getting critical security updates in a timely manner.

Rationale:

Google strongly recommends leaving this setting at the default (0 = Enable all variations), so fixes are gradually enabled (or if necessary, rapidly disabled) via the Chrome Variations framework.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Variations**
6. Ensure **Configuration** is set to **Enable Chrome variations**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Variations**
6. Set **Configuration** to **Enable Chrome variations**
7. Select **Save**









Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ChromeVariations>
2. https://support.google.com/chrome/a/answer/9805991?p=Manage_the_Chrome_variations_framework&_ga=2.161804159.274800631.1631808382-2031399475.1630502681&visit_id=637674174853642930-2644817764&rd=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.1.19 Other settings

2.3.1.19.1 (L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:

- Disabled (0): **Never send domain reliability data to Google**
- Enabled (1): **Domain Reliability data may be sent to Google depending on Chrome User Metrics (UMA) policy**

If the value for **DomainReliabilityAllowed** is not changed from the default, it will behave as it is enabled.

Rationale:

Setting this policy to disabled can stop any accidental data leakage.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow reporting of domain reliability related data**
6. Ensure **Configuration** is set to **Never send domain reliability data to Google**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Allow reporting of domain reliability related data**
6. Set **Configuration** to **Never send domain reliability data to Google**
7. Select **Save**






Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#DomainReliabilityAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

2.3.1.19.2 (L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows you to specify data types that will be limited/excluded from uploading data to the Google Chrome synchronization service.

The recommended state for this setting is: **Enabled** with the following text value **passwords** (Case Sensitive)

NOTE: Other settings in addition to **passwords** can be included based on organizational needs.

Rationale:

Storing and sharing information could potentially expose sensitive information, including but not limited to user passwords and login information. Allowing this synchronization could also potentially allow an end user to pull corporate data that was synchronized into the cloud to a personal machine.

Impact:

Password data will not be synchronized with the Google Chrome synchronization service.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync (ChromeOS)**
6. Ensure **Configuration** is set to **Allow Chrome Sync**
7. Ensure **List of types that should be excluded from synchronization** is set to **Passwords**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Under **User & browser settings**, select **Chrome Sync (ChromeOS)**
6. Set **Configuration** to **Allow Chrome Sync**
7. Set **List of types that should be excluded from synchronization** to **Passwords**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SyncTypesListDisabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2 Device Settings

The **Device Settings** section is where ChromeOS only configurations exist.

2.3.2.1 Enrollment and access

2.3.2.1.1 (L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy can force your organization's ChromeOS devices to re-enroll to your account after a device wipe. By default, a user is not required to enter a username and password for re-enrollment to occur. Re-enrollment ensures that your organization's ChromeOS devices remain managed, and that the policies you set are enforced on the device.

The three settings for this policy are:

- Force device to automatically re-enroll after wiping — ChromeOS devices automatically re-enroll into your organization's account after a wipe without user credentials being required.
- Force device to re-enroll with user credentials after wiping — A User must manually re-enroll ChromeOS devices into your account by logging in with their credentials.
- Device is not forced to re-enroll after wiping — The ChromeOS device is not re-enrolled into your organization's account and can be used without restrictions.

Note: When a ChromeOS device is being removed from service, or is no longer being managed through your organization, then the device should be [deprovisioned].(<https://support.google.com/chrome/a/answer/3523633?.sjid=10825622187269789335-NC>)

Rationale:

Requiring all devices to automatically re-enroll after a device wipe will keep your organization's ChromeOS devices managed. It is recommended to require user credentials to re-enroll the device. This requires a user within your organization to manually enter their credentials.

Note: ChromeOS devices that are being used in developer mode should not be forced to re-enroll. Creating an organization in the Google admin console for just those users will allow you to turn off forced re-enrollment.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Forced re-enrollment**
7. Ensure **Forced re-enrollment** is set to **Force device to re-enroll with user credentials after wiping**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Forced re-enrollment**
7. Set **Forced re-enrollment** to **Force device to re-enroll with user credentials after wiping**
8. Select **Save**

References:

1. <https://support.google.com/chrome/a/answer/6352858>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

2.3.2.1.2 (L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Powerwash allows a user to restore ChromeOS device to a factory state.

Allowing users to initiate a powerwash is the default.

Rationale:

Allowing a user to restore the ChromeOS device can remove any possibly malicious software that has been installed. Pairing this with forced re-enrollment allows the user to immediately re-enroll the device to your organization's account, after entering their credentials, so that it is properly managed.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Powerwash**
7. Ensure **Powerwash** is set to **Allow powerwash to be triggered**

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Powerwash**
7. Set **Powerwash** to **Allow powerwash to be triggered**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#DevicePowerwashAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.11 <u>Enforce Remote Wipe Capability on Portable End-User Devices</u> Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.			
v7	13.2 <u>Remove Sensitive Data or Systems Not Regularly Accessed by Organization</u> Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.			

2.3.2.1.3 (L2) Ensure 'Verified access' Is Set to 'Enable for content protection' (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Verified Access ensures that a device connecting to your network has been unmodified and is policy-compliant. Verified Access serves as an access point for a network service (such as a VPN gateway, a sensitive server, an enterprise Certificate Authority [CA], or an enterprise Wi-Fi access point) to get a hardware-backed cryptographic guarantee of the identity of the device and user that's trying to access it.

Verified Access uses the Trusted Platform Module (TPM) - present in every Chrome OS device - to enable enterprise network services to cryptographically confirm the identity and status of secure mode and enterprise policy using a Google server-side Application Programming Interface (API).

Rationale:

The Chrome Verified Access API allows network services, such as VPNs, intranet pages, and so on to cryptographically verify that their clients are genuine and conform to corporate policy. Most large enterprises have the requirement to allow only enterprise-managed devices onto their WPA2 EAP-TLS networks, higher-tier access in VPNs, and mutual-TLS intranet pages.

Impact:

This would impact a user that is required to use a development branch of ChromeOS.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Verified access**
7. Ensure **Verified access** is set to **Enable for content protection**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Verified access**
7. Set **Verified access** to **Enable for content protection**
8. Select **Save**





References:

1. <https://chromeenterprise.google/policies/#AttestationForContentProtectionEnabled>
2. <https://support.google.com/chrome/a/answer/7156268>

Additional Information:

To properly configure Verified Mode, your organization will need to create both a Chrome extension and a network service endpoint. To set up both the extension and the network service endpoint, follow the instructions in the [Chrome Verified Access Developer's Guide](#).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 <u>Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure</u> Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

2.3.2.1.4 Ensure 'Disabled device return instructions' Is Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls what text is displayed on a ChromeOS device that has been disabled due to loss or theft.

Rationale:

Instructions need to be created for how a disabled device is returned to your organization. A return address and contact phone number should be included in these instructions. This will alert anyone who sees the ChromeOS devices display that it needs to be returned.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Disabled device return instructions**
7. Ensure **Disabled device return instructions** is set to organization's return instructions

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Enrollment and access**, select **Disabled device return instructions**
7. Configure **Disabled device return instructions** to your organization's return instructions
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.2 Sign-in settings

2.3.2.2.1 (L1) Ensure 'Guest mode' Is Set to 'Disable guest mode' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

A guest login on ChromeOS is an anonymous user session where a password is not required. The **Guest mode** control allows an option to sign in as a guest on managed ChromeOS devices. When set to **Allow guest mode**, then the login screen will offer the ability to sign in as a guest user. When set to **Disable guest mode**, that option is removed from the login screen.

The default is **Disable guest mode** for K-12 EDU domains, and **Allow guest mode** on all others.

Rationale:

Removing the guest login option will not allow anonymous user sessions and will require each user to log in with their credentials.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Guest mode**
7. Ensure **Guest mode** is set to **Disable guest mode**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Guest mode**
7. Set **Guest mode** to **Disable guest mode**
8. Select **Save**






Default Value:

- **Disable guest mode** for K-12 EDU domains
- **Allow guest mode** on all other domains.

References:

1. <https://chromeenterprise.google/policies/#DeviceGuestModeEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

2.3.2.2.2 (L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy creates restrictions on who is allowed to sign into your organization's ChromeOS devices. If the policy is not configured, there is no restriction on who can sign into the device(s).

Rationale:

A list of users should be defined that are allowed to log into your organization's ChromeOS devices.

Impact:

This should not impact the users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Sign-in restriction**
7. Ensure **Sign-in restriction** is set to **Restrict sign-in to a list of users**
8. Ensure **Allowed users** is configured to your organization's requirements

Remediation:







To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Sign-in restriction**
7. Set **Sign-in restriction** to **Restrict sign-in to a list of users**
8. Set **Allowed users** to your organization's requirements
9. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#DeviceAllowNewUsers>
2. <https://chromeenterprise.google/policies/#DeviceUserAllowlist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.2 <u>Establish and Maintain a Data Inventory</u> Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

2.3.2.2.3 (L2) Ensure 'Sign-in screen' Is Set to 'Never show user names and photos' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy configures whether the sign-in screen on your organization's ChromeOS devices display names and pictures of users who have signed in previously.

Rationale:

All users are required to sign into the ChromeOS device with their credentials, and names and pictures should not be displayed. This prevents anyone who accesses the device to know who is either with your organization or who has signed in previously on the device.

Impact:

This may make logging into the ChromeOS device more difficult for certain users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Sign-in screen**
7. Ensure **Sign-in screen** is set to **Never show user names and photos**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Sign-in screen**
7. Set **Sign-in screen** to **Never show user names and photos**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#DeviceShowUserNamesOnSignin>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.2.4 (L1) Ensure 'User data' Is Set to 'Do not erase local user data' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether ChromeOS devices are switched to ephemeral mode. In ephemeral mode, local user data is saved on disk for the length of the session and then the data is deleted after the session is over. No data is therefore saved to the device.

The recommended state for this setting is: **Do not erase local user data**

Note: When set to **Do not erase local user data**, all local user data is encrypted on device.

Rationale:

Allowing use of ephemeral profiles allows a user to use Google ChromeOS with no data being logged to the system. Deleting local user data will delete information that may be important for a computer investigation, and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **User data**
7. Ensure **User data** is set to **Do not erase local user data**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **User data**
7. Set **User data** to **Do not erase local user data**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#DeviceEphemeralUsersEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.2.5 (L1) Ensure 'Privacy screen on sign-in screen' Is Set to 'Always enable the privacy screen on sign-in screen' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The privacy screen for ChromeOS is a feature that activates when the user walks away from the Chromebook. If activated, the screen will dim after 10 seconds. It can also keep the screen awake while the user is in front of the Chromebook even if they are not interacting with the device.

This policy requires ChromeOS devices with both a built-in webcam and an integrated electronic privacy screen.

Rationale:

Setting the operating system to automatically dim and lock the screen when the user moves away from the device protects potentially sensitive user data.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Privacy screen on sign-in screen**
7. Ensure **Privacy screen on sign-in screen** is set to **Always enable the privacy screen on sign-in screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Privacy screen on sign-in screen**
7. Set **Privacy screen on sign-in screen** to **Always enable the privacy screen on sign-in screen**
8. Select **Save**

Default Value:

If this policy is left unset, the privacy screen is disabled initially, but remains controllable by the user when the login screen is shown.

References:

1. <https://chromeenterprise.google/policies/#DeviceLoginScreenPrivacyScreenEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.2.6 (L1) Ensure 'Show numeric keyboard for password' Is Set to 'Default to a standard keyboard for password input' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether ChromeOS displays a numeric keyboard or a standard keyboard on the login screen. The two configuration options are:

- Default to a numeric keyboard for password input
- Default to a standard keyboard for password input

Rationale:

Users are not allowed to use a strictly numeric password to sign in, therefore the policy should require a standard keyboard. This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Show numeric keyboard for password**
7. Ensure **Show numeric keyboard for password** is set to **Default to a standard keyboard for password input**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Sign-in settings**, select **Show numeric keyboard for password**
7. Set **Show numeric keyboard for password** to **Default to a standard keyboard for password input**
8. Select **Save**

Default Value:

Unset (false) - show standard keyboard

References:

1. <https://chromeenterprise.google/policies/#DeviceShowNumericKeyboardForPassword>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.3 Device update settings

2.3.2.3.1 Auto-update settings

ChromeOS devices should be properly configured to update automatically.

2.3.2.3.1.1 (L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls the automatic updating of ChromeOS.

Rationale:

Automatic updates should be enabled.

Impact:

There should be no impact to the user.

Audit:

To verify this setting via the Google Workspace Admin Console:







1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Allow devices to automatically update OS version** is set to **Allow updates**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Allow devices to automatically update OS version** to **Allow updates**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

2.3.2.3.1.2 (L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3 (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy configures what versions of ChromeOS are allowed in your organization.

Rationale:

The target version for ChromeOS should be no less than the current version and the preceding three versions.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:







1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Target version** is set to the current version of ChromeOS or one of the three previous versions

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Target version** to the current version of ChromeOS or one of the three previous versions
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

2.3.2.3.1.3 (L2) Ensure 'Roll back to target version' Is Set to 'Do not roll back OS' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls if ChromeOS versions can be rolled back to a previous version.

Rationale:

ChromeOS updates should not be rolled back due to possible security issues in previous versions.

Impact:

This might cause an issue where a user has an extension that is not compatible with the newest version of ChromeOS.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Roll back to target version** is set to **Do not roll back OS**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Roll back to target version** to **Do not roll back OS**
8. Select **Save**

References:

1. https://support.google.com/chrome/a/answer/12569990?visit_id=638590849717719184-3325755204&p=rollback&rd=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.3.1.4 (L1) Ensure 'Release channel' Is Set to 'Stable channel' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls what update release channel your organization's ChromeOS devices follow.

Rationale:

Standard user ChromeOS devices should be on the stable release channel.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Release channel** is set to **Stable channel**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Release channel** to **Stable channel**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.3.1.5 (L1) Ensure 'Rollout plan' Is Configured (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy configures how updates are rolled out in your organization.

Rationale:

Your organization should determine how update rollout happens.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:






1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Rollout plan** is configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Rollout plan** to your organization's requirements
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.4 <u>Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

2.3.2.3.1.6 (L2) Ensure 'Peer to peer' Is Set to 'Do not allow peer to peer auto update downloads' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls whether ChromeOS devices are allowed to update via peer-to-peer connections.

Rationale:

Updates should only be downloaded from Google's servers. Updating from another ChromeOS device could allow malicious content to be loaded.

Impact:

There should be no impact to the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Peer to peer** is set to **Do not allow peer to peer auto update downloads**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Peer to peer** to **Do not allow peer to peer auto update downloads**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	15.6 <u>Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients</u> Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.		●	●

2.3.2.3.1.7 (L2) Ensure 'Enforce updates' Is Configured (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy set controls how devices and users are handled when running a version of ChromeOS that is outside the required version(s).

Rationale:

This policy set should be configured to your organization's requirements.

Impact:

Only ChromeOS devices that are running a version outside the required version(s) would be affected.

Audit:

To verify this setting via the Google Workspace Admin Console:







1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Enforce updates** is configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Enforce updates** to match your organization's requirements
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

2.3.2.3.1.8 Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether updates can be downloaded over HTTPS only or also with HTTP.

Rationale:

Updates should only be downloaded on a secure connection.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:




1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Ensure **Update downloads** is set to **Use HTTPS for update downloads**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Edit in legacy view** beside **Auto-update settings**
7. Set **Update downloads** to **Use HTTPS for update downloads**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

2.3.2.3.2 (L1) Ensure 'Variations' Is Set to 'Enable Chrome variations' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Configuring this setting allows specifying which variations are allowed to be applied in Google Chrome. Variations provide a means for Google to offer modifications to Google Chrome without shipping a new version of the browser by selectively enabling or disabling already existing features.

- **Enable all variations**: Allows all variations to be applied to the browser (Default value).
- **Enable variations concerning critical fixes only**: Allows only variations considered critical security or stability fixes to be applied to Google Chrome.
- **Disable all variations**: Prevent all variations from being applied to the browser. Please note that this mode can potentially prevent the Google Chrome developers from providing critical security fixes in a timely manner and is thus not recommended.

The recommended state for this setting is: **Enable all variations**

NOTE: Google strongly believes there is no added security benefit for turning this to critical fixes, as leaving it on increases the stability of the browser. Disabling variations can also prevent getting critical security updates in a timely manner.

Rationale:

Google strongly recommends leaving this setting at the default (0 = Enable all variations), so fixes are gradually enabled (or if necessary, rapidly disabled) via the Chrome Variations framework.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Variations**
7. Ensure **Variations** is set to **Enable Chrome variations**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Device update settings**, select **Variations**
7. Set **Variations** to **Enable Chrome variations**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ChromeVariations>
2. https://support.google.com/chrome/a/answer/9805991?p=Manage_the_Chrome_variations_framework&_ga=2.161804159.274800631.1631808382-2031399475.1630502681&visit_id=637674174853642930-2644817764&rd=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.4 User and device reporting

2.3.2.4.1 (L1) Ensure 'Metrics reporting' Is Set to 'Never send metrics to Google' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy allows Google ChromeOS to report data back to Google. That data is made up of diagnostic data, crash reports, and usage metrics. It does not include web page URLs or any personal information except in crash reports. Depending on what was happening at the time of the crash, the crash report contains system information at the time of the crash and might contain webpage URLs or personal information.

Rationale:

Sending any data to an organization outside of your own, even aggregated, could lead to data leakage and should be avoided.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Metrics reporting**
7. Ensure **Metrics reporting** is set to **Never send metrics to Google**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Metrics reporting**
7. Set **Metrics reporting** to **Never send metrics to Google**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#DeviceMetricsReportingEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.2.4.2 (L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether system logs are uploaded to the management server. The default is unset or no system logs are reported.

Rationale:

System logs should be uploaded to allow your organization's admins to monitor system logs.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Device system log upload**
7. Ensure **Device system log upload** is set to **Enable device system log upload**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Device system log upload**
7. Set **Device system log upload** to **Enable device system log upload**
8. Select **Save**






Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#LogUploadEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

2.3.2.5 Other settings

2.3.2.5.1 (L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls whether system traffic can go through an internet proxy server with authentication.

Rationale:

The default to block system traffic from going through a proxy with authentication keeps users from providing credentials to a possibly malicious proxy server.

Impact:

This might block a device from access the internet from known good proxy servers.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Authenticated Proxy Traffic**
7. Ensure **Authenticated Proxy Traffic** is set to **Block system traffic from going through a proxy server with authentication**

Remediation:




To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **User and device reporting**, select **Authenticated Proxy Traffic**
7. Set **Authenticated Proxy Traffic** to **Block system traffic from going through a proxy server with authentication**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#SystemProxySettings>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.3 <u>Deploy a Network Intrusion Detection Solution</u> Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.			
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

2.3.2.5.2 (L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether the AES Keylocker implementation is enabled for local user storage. This policy only applies to user homes which use dm-crypt for encryption. Legacy home users, those that do not use dm-crypt, are not supported and will default to AESNI (or disabled).

Rationale:

User home folders should be encrypted using AES Keylocker where applicable.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Other settings**, select **Enable Key Locker**
7. Ensure **Enable Key Locker** is set to **Use Key Locker with the encryption algorithm for user storage encryption, if supported**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Other settings**, select **Enable Key Locker**
7. Set **Enable Key Locker** to **Use Key Locker with the encryption algorithm** for user storage encryption, if supported
8. Select **Save**




Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#DeviceKeylockerForStorageEncryptionEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

2.3.2.6 Security

2.3.2.6.1 (L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This configures whether Google Chrome will offer a post-quantum key agreement algorithm in TLS, using the ML-KEM NIST standard, and will protect user traffic from quantum computers when communicating with compatible servers. Enabling a post-quantum key agreement is backwards compatible, so there will be no issue with existing TLS servers.

Rationale:

This will protect user traffic from quantum computer decrypting.

Impact:

There should be no impact on the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Security**, select **Post-quantum TLS**
7. Ensure **Configuration** is set to **Allow post-quantum key agreement in TLS connections**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Device settings**
6. Under **Security**, select **Post-quantum TLS**
7. Set **Configuration** to **Allow post-quantum key agreement in TLS connections**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PostQuantumKeyAgreementEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3 Managed guest session settings

These configurations settings are for ChromeOS devices that are allowing guest sessions.

2.3.3.1 General

2.3.3.1.1 (L1) *Ensure 'Managed guest session' Is Configured (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Managed guest sessions allow multiple users to share the same ChromeOS device without having to sign in to their Google Account. This should be used for ChromeOS devices as loaner devices or shared computers.

Managed guest sessions allow users to have a full browsing experience and access multiple websites in windowed mode but not in full-screen.

Rationale:

If your organization uses guest sessions on Google ChromeOS, this policy should be configured to meet your organization's requirements.

Impact:

There should be no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Managed guest session**
7. Ensure **Managed guest session** is set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Managed guest session**
7. Set **Managed guest session** to your organization's requirements
8. Select **Save**

References:

1. <https://support.google.com/chrome/a/answer/3017014?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3.3.1.2 (L1) Ensure 'Maximum user session length' Is Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This control sets the length of time that a session can run before the user is logged out and the session is terminated. The user is shown in the system tray how much time is remaining before they will be automatically logged out.

The values are between 1 minute to 1440 minutes. If no value is set, then the system observes an unlimited session time.

While 60 minutes is a good operating baseline for the session, depending on your organization this may vary. For example, in K-12 a 24 hour (1440 minutes) session might be the best setting. Use the best setting for your organization's needs.

Rationale:

Setting a session length allows ChromeOS to not have a user session always signed in and cannot be immediately accessed by someone other than the user.

Impact:

There could be impact to the user if they are unaware, or not checking, the session timer, and they are logged out.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Maximum user session length**
7. Ensure **Maximum session length** is set to your organization's parameters

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Maximum user session length**
7. Set **Maximum session length** to your organization's parameters
8. Select **Save**

Default Value:

Unset (Unlimited session length)

References:

1. <https://chromeenterprise.google/policies/#SessionLengthLimit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.1 Maintain an Inventory of Authentication Systems Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.		●	●

2.3.3.1.3 (L1) *Ensure 'Custom terms of service' Is Configured (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Impact:

If users are not informed of their responsibilities, unapproved activities may occur. Users that are not approved for access may take the lack of a warning banner as implied consent to access.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Custom terms of service**
7. Ensure a **.txt** or **.text** file has been uploaded that contains your organization's custom terms of service

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **General**, select **Custom terms of service**
7. Select **Upload**
8. Select a **.txt** or **.text** file from your local device that contains your organization's custom terms of service
9. Select **Save**

Default Value:

Unset

References:

1. <https://chromeenterprise.google/policies/#TermsOfServiceURL>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.2 Apps and extensions

2.3.3.2.1 (L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Task Manager in ChromeOS allows the user to kill any current processes running.

Rationale:

If the Task Manager is enabled, a user can kill any running task, including those that your organization uses to manage the user of the device. Disabling that functionality removes this possibility.

Impact:

If a task is no longer responding, the user would have to turn the device off and back on to kill that task.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Apps and extensions**, select **Task manager**
7. Ensure **Task manager** is set to **Block users from ending processes with the Chrome task manager**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Apps and extensions**, select **Task manager**
7. Set **Task manager** to **Block users from ending processes with the Chrome task manager**
8. Select **Save**

Default Value:

Unset (same as enabled)

References:

1. <https://chromeenterprise.google/policies/#TaskManagerEndProcessEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.2.2 (L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls extension management settings for Google Chrome, specifically v2 extensions. This policy setting is being sunsetted as Google develops the Manifest v3, but that rollout is currently postponed.

The policy can be configured to:

- Default browser behavior
- Manifest v2 is disabled
- Manifest v2 is enabled
- Manifest v2 is enabled for forced extensions only

Rationale:

Setting this to Forced Only will not allow users to install any additional v2 extensions, and all existing, non-forced, v2 extensions will be disabled.

Impact:

Users that use extensions regularly will have a set of them blocked, which will change their user experience.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Apps and extensions**, select **Manifest v2 extension availability**
7. Ensure **Configuration** is set to **Enable force-installed manifest v2 extensions on the sign-in screen**

Remediation:







To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Apps and extensions**, select **Manifest v2 extension availability**
7. Set **Configuration** to **Enable force-installed manifest v2 extensions on the sign-in screen**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ExtensionManifestV2Availability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 <u>Establish and Maintain a Remediation Process</u> Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.3.3.3 Security

2.3.3.3.1 (L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the WebAuthn API and its interaction with sites that have a broken TLS certificate. It can be configured to either:

- Do not allow WebAuthn API requests on sites with broken TLS certificates.
- Allow WebAuthn API requests on sites with broken TLS certificates.

Rationale:

Setting this policy will block the ability to authenticate to any website that does not have a valid TLS certificate since the identity of the site cannot be verified.

Impact:

There should be no user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Web Authentication requests on sites with broken TLS certificates**
7. Ensure **Web Authentication requests on sites with broken TLS certificates** is set to **Do not allow WebAuthn API requests on sites with broken TLS certificates**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Web Authentication requests on sites with broken TLS certificates**
7. Set **Web Authentication requests on sites with broken TLS certificates** to **Do not allow WebAuthn API requests on sites with broken TLS certificates**
8. Select **Save**





Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#AllowWebAuthnWithBrokenTlsCerts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3.3.2 (L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for Google Chrome to allow legacy or insecure hashes during the TLS handshake. It can be configured to either:

- Do Not Allow Insecure Hashes in TLS Handshakes
- Allow Insecure Hashes in TLS Handshakes

If the value for `InsecureHashesInTLSHandshakesEnabled` is not changed from the default, it will behave as if it is enabled.

Rationale:

Setting this policy to disabled will block Google Chrome from using insecure hashes. Using insecure, or legacy, hashes could allow sensitive data to be exposed.

Impact:

Users would be blocked from visiting sites that do not support more secure hashes.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Insecure hashes in TLS handshakes**
7. Ensure **Insecure hashes in TLS handshakes** is set to **Do not allow insecure hashes in TLS handshakes**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Insecure hashes in TLS handshakes**
7. Set **Insecure hashes in TLS handshakes** to **Do not allow insecure hashes in TLS handshakes**
8. Select **Save**





Default Value:

Unset (Allow)

References:

1. <https://chromeenterprise.google/policies/#InsecureHashesInTLSHandshakesEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3.3.3 (L1) *Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This configures whether Google Chrome will offer a post-quantum key agreement algorithm in TLS, using the ML-KEM NIST standard, and will protect user traffic from quantum computers when communicating with compatible servers. Enabling a post-quantum key agreement is backwards compatible, so there will be no issue with existing TLS servers.

Rationale:

This will protect user traffic from quantum computer decrypting.

Impact:

There should be no impact on the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Post-quantum TLS**
7. Ensure **Configuration** is set to **Allow post-quantum key agreement in TLS connections**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Post-quantum TLS**
7. Set **Configuration** to **Allow post-quantum key agreement in TLS connections**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PostQuantumKeyAgreementEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3.3.4 (L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Specifies whether the user may open pages in Incognito mode in Google Chrome. The possible values are:

- Incognito mode available
- Incognito mode disabled
- Incognito mode forced

The recommended state for this setting is: Incognito mode disabled

Rationale:

Incognito mode in Chrome gives you the choice to browse the internet without your activity being saved to your browser or device.

Allowing users to use the browser without any information being saved can hide evidence of malicious behaviors. This information may be important for a computer investigation, and investigators such as Computer Forensics Analysts may not be able to retrieve pertinent information to the investigation.

Impact:

Users will not be able to initiate Incognito mode for Google Chrome.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select Devices
3. Select Chrome
4. Select Settings
5. Select Managed guest session settings
6. Under Security, select Incognito mode
7. Ensure Incognito mode is set to Disallow incognito mode

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Incognito mode**
7. Set **Incognito mode** to **Disallow incognito mode**
8. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#IncognitoModeAvailability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.3.5 (L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google ChromeOS is configured to save the browser history.

The recommended state for this setting is: **Always save browser history**

NOTE: This setting will preserve browsing history that could contain a user's personal browsing history. Please make sure that this setting is in compliance with organizational policies.

Rationale:

Browser history shall be saved as it may contain indicators of compromise.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Browser history**
7. Ensure **Browser history** is set to **Always save browser history**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Browser history**
7. Set **Browser history** to **Always save browser history**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change).

References:

1. <https://chromeenterprise.google/policies/#SavingBrowserHistoryDisabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

2.3.3.3.6 (L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the defaults for using Encrypted ClientHello (ECH). ECH is an extension to TLS and encrypts the initial handshake with a website that can only be decrypted by that website. Google Chrome may, or may not, use ECH based on 3 factors: server support, HTTPS DNS record availability, or rollout status. It can be configured to either:

- Disable the TLS Encrypted ClientHello experiment
- Enable the TLS Encrypted ClientHello experiment

If the value for `EncryptedClientHelloEnabled` is not changed from the default, it will behave as though it is enabled.

Rationale:

Previously all handshakes were in the open and could expose sensitive information, such as the name of the website to which you are connecting. Setting this policy will allow Google Chrome to use an encrypted hello, or handshake, with a website where it is supported, thus not exposing sensitive information.

Impact:

There should be no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **TLS encrypted ClientHello**
7. Ensure **Configuration** is set to **Enable the TLS Encrypted ClientHello experiment**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **TLS encrypted ClientHello**
7. Set **Configuration** to **Enable the TLS Encrypted ClientHello experiment**
8. Select **Save**





Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#EncryptedClientHelloEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3.3.7 (L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for Google Chrome to upgrade to HTTPS from HTTP while navigating to certain sites. It can be configured to either:

- Scripts for workers (Web Workers, Service Workers, etc.) use lax MIME type checking. Worker scripts with legacy MIME types, like text/ascii, will work.
- Scripts for workers (Web Workers, Service Workers, etc.) require a JavaScript MIME type, like text/javascript. Worker scripts with legacy MIME types, like text/ascii, will be rejected.

If the default is not changed, it will behave as if it is enabled.

Rationale:

Setting this policy will require worker scripts to use more secure and strict JavaScript MIME types and ones with legacy MIME Types will be rejected.

Impact:

This should have no impact on users.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Strict MIME type checking for worker scripts**
7. Ensure **Configuration** is set to **Require a JavaScript MIME type for worker scripts**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Strict MIME type checking for worker scripts**
7. Set **Configuration** to **Require a JavaScript MIME type for worker scripts**
8. Select **Save**

Default Value:

Unset (Enabled)

References:

1. <https://chromeenterprise.google/policies/#StrictMimetypeCheckForWorkerScriptsEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.3.3.8 (L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the ability for the file/directory picker to be called without user interaction.

If the value is not changed from the default, it will behave as if it is disabled.

Rationale:

Setting this policy would allow the URLs selected to call the the file or directory picker web APIs without any user gesture/interaction. This policy does not need to be set for this reason.

Impact:

Disabling this policy should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **File/directory picker without user gesture**
7. Ensure **Allow file or directory picker APIs to be called without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **File/directory picker without user gesture**
7. Remove all URLs from **Allow file or directory picker APIs to be called without prior user gesture**
8. Select **Save**







Default Value:

Unset (Disabled)

References:

1. <https://chromeenterprise.google/policies/#FileOrDirectoryPickerWithoutGestureAllowedForOrigins>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 Establish and Maintain a Remediation Process Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

2.3.3.3.9 (L1) Ensure 'Media picker without user gesture' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls if URLs or hostname patterns can display the media picker for a screen capture without user interaction.

Rationale:

To call the media picker, a prior gesture from a user needs to be required. If there is no user gesture then the call will fail.

Impact:

None - this is the default.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Media picker without user gesture**
7. Ensure **Allow screen capture without prior user gesture** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Security**, select **Media picker without user gesture**
7. Remove all URLs from **Allow screen capture without prior user gesture**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.4 Remote access

2.3.3.4.1 (L1) *Ensure 'Remote access clients' Is Configured (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls what client domain names have remote access to the client ChromeOS devices in your organization. Only a connection from one of the specified client domains can connect to the client device.

Leaving the policy empty (or unsetting it) applies the default policy for the connection type. For remote assistance, this allows clients from any domain to connect to the host. For anytime remote access, only the host owner can connect.

Rationale:

Your organization should configure **Remote access clients** for the client domains in your organization that have access to your client devices.

Impact:

There should be no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote access clients**
7. Ensure **Remote access client domain** is set to your organization's requirements

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote access clients**
7. Set **Remote access client domain** to your organization's requirements
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostClientDomainList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 <u>Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure</u> Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.			
v7	12.1 <u>Maintain an Inventory of Network Boundaries</u> Maintain an up-to-date inventory of all of the organization's network boundaries.			

2.3.3.4.2 (L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Chrome allows the configuration of a list of domains that are allowed to access the user's system. When enabled, remote systems can only connect if they are one of the specified domains listed.

Setting this to an empty list (Disabled) allows remote systems from any domain to connect to this user's system.

The recommended state for this setting is: **Enabled** (1) and at least one domain set.

NOTE: The list of domains is organization-specific.

Rationale:

Remote assistance connections shall be restricted.

Impact:

If this setting is enabled, only systems from the specified domains can connect to the user's system.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote access hosts**
7. Ensure **Remote access host domain** is set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote access hosts**
7. Set **Remote access host domain** to your organization's requirements
8. Select **Save**




Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostDomainList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.3.4.3 (L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome allows the use of relay servers when clients are trying to connect to this machine and a direct connection is not available.

- The use of relay servers by the remote access host is not allowed
- The use of relay servers by the remote access host is allowed

The recommended state for this setting is: The use of relay servers by the remote access host is not allowed

Rationale:

Relay servers shall not be used to circumvent firewall restrictions.

Impact:

If this setting is disabled, remote clients can not use relay servers to connect to this machine.

NOTE: Setting this to Disabled doesn't turn remote access off, but only allows connections from the same network (not NAT traversal or relay).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Firewall traversal**
7. Ensure **Firewall traversal** is set to **Disable the use of relay servers**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Firewall traversal**
7. Set **Firewall traversal** to **Disable the use of relay servers**
8. Select **Save**




Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRelayedConnection>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.3.4.4 (L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This is a setting for Chrome Remote desktop. If this setting is Disabled, the remote access host service cannot be started or configured to accept incoming connections.

- Prevent remote access connections to this machine
- Allow remote access connections to this machine

The recommended state for this setting is: Prevent remote access connections to this machine

Rationale:

Only approved remote access systems should be used.

NOTE: If Chrome Remote Desktop is approved and required for use, then this setting can be ignored.

Impact:

This setting will disable Chrome Remote Desktop. In general, Chrome Remote Desktop is not used by most businesses, so disabling it should have no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote support connections**
7. Ensure **Remote support connections** is set to **Prevent remote support connections**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Remote access**, select **Remote support connections**
7. Set **Remote support connections** to **Prevent remote support connections**
8. Select **Save**




Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#RemoteAccessHostAllowRemoteAccessConnections>
2. <https://remotedesktop.google.com/?pli=1>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

2.3.3.5 Session settings

2.3.3.5.1 (L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The **Show sign-out button in tray** policy controls whether a sign-out button is in the system tray while the screen is not locked and the session is active.

Rationale:

Enabling the sign-out button in the system tray would allow a user to quickly log out of a session in a situation where there may be malicious actors trying to 'shoulder-surf' or to capture data from the user's screen.

Impact:

This would have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Session settings**, select **Show sign-out button in tray**
7. Ensure **Show sign-out button in tray** is set to **Show sign-out button in tray**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Session settings**, select **Show sign-out button in tray**
7. Set **Show sign-out button in tray** to **Show sign-out button in tray**
8. Select **Save**




Default Value:

Unset, no sign-out button.

References:

1. <https://chromeenterprise.google/policies/#ShowLogoutButtonInTray>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.6 Network

2.3.3.6.1 (L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers the functionality to configure the proxy settings by automatic discovery using WPAD (Web Proxy Auto-Discovery Protocol). Setting this configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified from the command line.

Disabled (0): Lets users choose their proxy settings.

The recommended state for this setting is: **Enabled** and the value of **ProxyMode** is not set to **auto_detect**

Rationale:

Attackers may abuse the WPAD auto-config functionality to supply computers with a PAC file that specifies a rogue web proxy under their control.

Impact:

If the policy is enabled, the proxy configuration will no longer be discovered using WPAD.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Proxy mode**
7. Ensure **Proxy mode** is not set to **Always auto detect the proxy**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Proxy mode**
7. Set **Proxy mode** to a setting other than **Always auto detect the proxy**
8. Select **Save**

Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#ProxySettings>
2. http://www.ptsecurity.com/download/wpad_weakness_en.pdf
3. <https://www.blackhat.com/us-16/briefings.html#crippling-https-with-unholy-pac>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●
v7	12.9 Deploy Application Layer Filtering Proxy Server Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●

2.3.3.6.2 (L2) *Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Manual)*

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy configures the ability for Google ChromeOS to bypass any proxy for captive portal authentication.

If enabled, these authentication webpages, starting from the captive portal sign-in page until Chrome detects a successful internet connection, will open in a separate window and ignore all policy settings and restrictions for the current user.

If disabled, any captive portal authentication pages are shown in a new browser tab that uses the current user's proxy settings.

This policy only takes effect if a proxy is set up (by policy, extension, or the user in chrome://settings).

Rationale:

Enabling captive portal sites to bypass proxy settings could grant access to the system from a malicious (or misconfigured) captive portal site. Setting the policy to disabled forces all sites, including captive portal sites, to use the configured proxy settings.

Impact:

This may impact a user's access to certain captive portal sites that do not work with the configured proxy server.

Audit:

To verify this setting via the Google Workspace Admin Console:





1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Ignore proxy on captive portals**
- 7 Ensure **Ignore proxy on captive portals** is set to **Keep policies for captive portal pages**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Ignore proxy on captive portals**
7. Set **Ignore proxy on captive portals** to **Keep policies for captive portal pages**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	15.1 <u>Maintain an Inventory of Authorized Wireless Access Points</u> Maintain an inventory of authorized wireless access points connected to the wired network.			

2.3.3.6.3 (L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls whether a user is able to proceed to a webpage when an invalid SSL certificate warning has occurred.

The recommended state for this setting is: **Block users from clicking through SSL warnings**

Rationale:

Sites protected by SSL should always be recognized as valid in the web browser. Allowing a user to make the decision as to whether there appears to be an invalid certificate could open an organization up to users visiting a site that is otherwise not secure and/or malicious in nature.

Impact:

Users will not be able to click past the invalid certificate error to view the website.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **SSL error override**
7. Ensure **SSL error override** is set to **Block users from clicking through SSL warnings**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **SSL error override**
7. Set **SSL error override** to **Block users from clicking through SSL warnings**
8. Select **Save**





Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SSLErrorOverrideAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.6.4 (L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This controls the mode of the DNS-over-HTTPS resolver. Please note that this setting will only set the default mode for each query. The mode may be overridden for special types of queries, such as requests to resolve a DNS-over-HTTPS server hostname.

- **Disable DNS-over-HTTPS** (off)
- **Enable DNS-over-HTTPS with insecure fallback** (automatic) - Enable DNS-over-HTTPS queries first if a DNS-over-HTTPS server is available and may fallback to sending insecure queries on error.
- **Enable DNS-over-HTTPS without insecure fallback** (secure) - Only send DNS-over-HTTPS queries and will fail to resolve on error.

The recommended state for this setting is: **Enabled** with a value of **Enable DNS-over-HTTPS without insecure fallback** (secure)

Note: When enabling this policy, it is recommended to also configure the **DnsOverHttpsTemplates** policy so that the URI templates are set. You can find out more information on the [DnsOverHttpsTemplates enterprise policy site](#).

Rationale:

DNS over HTTPS (DOH) has a couple primary benefits:

1. Encrypting DNS name resolution traffic helps to hide your online activities, since DoH hides the name resolution requests from the ISP and from anyone listening on intermediary networks.
2. DoH also helps to prevent DNS spoofing and man-in-the-middle (MitM) attacks.

Impact:

Not all DNS providers support DOH, so choice is limited. Also, Enterprises sometimes monitor DNS requests to block access to malicious or inappropriate sites. DNS monitoring can also sometimes be used to detect malware attempting to "phone home." Because DoH encrypts name resolution requests, it can create a security monitoring blind spot.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **DNS over HTTPS**
7. Ensure **DNS over HTTPS** is set to **Enable DNS-over-HTTPS without insecure fallback**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **DNS over HTTPS**
7. Set **DNS over HTTPS** to **Enable DNS-over-HTTPS without insecure fallback**
8. Select **Save**





Default Value:

Unset (Same as Enable DNS-over-HTTPS with insecure fallback (automatic)). If any policy is set, either through being domain-joined or active policy with cloud management (or profile lists), then it sometimes reverts to Disable DNS-over-HTTPS and users can't change it.

References:

1. <https://chromeenterprise.google/policies/#DnsOverHttpsMode>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.3.6.5 (L1) Ensure 'SharedArrayBuffer' Is Set to 'Prevent sites that are not cross-origin isolated from using SharedArrayBuffers' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether SharedArrayBuffers can be used in a non cross-origin-isolated context.

Rationale:

Sites that are not cross-origin isolated need to be prevented from using the SharedArrayBuffers.

Impact:

There should be no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **SharedArrayBuffer**
7. Ensure **SharedArrayBuffer** is set to **Prevent sites that are not cross-origin isolated from using SharedArrayBuffers**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **SharedArrayBuffer**
7. Set **SharedArrayBuffer** to **Prevent sites that are not cross-origin isolated from using SharedArrayBuffers**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#SharedArrayBufferUnrestrictedAccessAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.6.6 (L1) Ensure 'Globally scoped HTTP authentication cache' is set to 'HTTP authentication credentials are scoped to top-level sites' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether HTTP auth credentials may be automatically used in the context of another web site visited in Google Chrome.

The recommended state for this setting is: **HTTP authentication credentials are scoped to top-level sites**

NOTE: This setting is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future.

Rationale:

Allowing HTTP auth credentials to be shared without the user's consent could lead to a user sharing sensitive information without their knowledge. Enabling this setting could also lead to some types of cross-site attacks that would allow users to be tracked across sites without the use of cookies.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Globally scoped HTTP authentication cache**
7. Ensure **Globally scoped HTTP authentication cache** is set to **Block cross-origin authentication**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Globally scoped HTTP authentication cache**
7. Set **Globally scoped HTTP authentication cache** to **HTTP authentication credentials are scoped to top-level sites**
8. Select **Save**

Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#GloballyScopeHTTPAuthCacheEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.6.7 (L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows a list of names to be specified that will be exempt from HTTP Strict Transport Security (HSTS) policy checks, then potentially upgraded from http:// to https://.

The recommended state for this setting is not configured.

Rationale:

Allowing hostnames to be exempt from HSTS checks could allow for protocol downgrade attacks and cookie hijackings.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **HSTS policy bypass list**
7. Ensure **List of hostnames that will bypass the HSTS policy check** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **HSTS policy bypass list**
7. Remove all hostnames from **List of hostnames that will bypass the HSTS policy check**
8. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#HSTSPolicyBypassList>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.6.8 (L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines whether a local switch is configured for DNS interception checks. These checks attempt to discover if the browser is behind a proxy that redirects unknown host names.

The recommended state for this setting is: **Perform DNS interception checks**

NOTE: This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on startup and each DNS configuration change.

Rationale:

Disabling these checks could potentially allow DNS hijacking and poisoning.

Impact:

None - This is the default behavior.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **DNS interception checks enabled**
7. Ensure **DNS interception checks enabled** is set to **Perform DNS interception checks**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **DNS interception checks enabled**
7. Set **DNS interception checks enabled** to **Perform DNS interception checks**
8. Select **Save**





Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DNSInterceptionChecksEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.7 Remediate Detected Vulnerabilities Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.			
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			

2.3.3.7 Content

2.3.3.7.1 (L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting ensures that web search results with Google are performed with SafeSearch set to always active. Disabled means SafeSearch in Google Search is not enforced.

The recommended state for this setting is: **Enabled** (1)

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are more prone to malicious content, including spyware, adware, and viruses.

Impact:

User search results will be filtered and content such as adult text, videos, and images will not be shown.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **SafeSearch and Restricted Mode**
7. Ensure **SafeSearch and Restricted Mode** is set to **Always use Safe Search for Google Web Search queries**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **SafeSearch and Restricted Mode**
7. Set **SafeSearch and Restricted Mode** to **Always use Safe Search for Google Web Search queries**
8. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ForceGoogleSafeSearch>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.7.2 (L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the defaults for clipboard permission access from sites. It can be configured to either:

- Allow the user to decide
- Allow sites to ask the user to grant the clipboard site permission
- Do not allow any site to use the clipboard site permission

Rationale:

The clipboard stores data, text, and images that are shared between all applications. An organization would disable clipboard access to restrict sites from reading the contents of the clipboard when visiting.

Impact:

Not allowing sites to have access to the clipboard permission can cause issues with formatting or access to needed images on the clipboard.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Clipboard**
7. Ensure **Clipboard** is set to **Do not allow any site to use the clipboard site permission**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Clipboard**
7. Set **Clipboard** to **Do not allow any site to use the clipboard site permission**
8. Select **Save**

Default Value:

Allow clipboard permission access

References:

1. <https://chromeenterprise.google/policies/#DefaultClipboardSetting>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.7.3 (L1) *Ensure 'Auto open downloaded files' Is Not Set (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls whether specified file types are allowed to auto open on download. It also controls specified URLs to allow those specified file types to auto open when they are downloaded from those URLs.

Rationale:

No file types should not be allowed to auto open and the user is required to interact with every downloaded file they wish to open.

Impact:

There is no impact to the user

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Auto open downloaded files**
7. Ensure **Auto open file types** is not configured
8. Ensure **Auto open URLs** is not configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Auto open downloaded files**
7. Remove all file types from **Auto open file types**
8. Remove all URLs from **Auto open URLs**
9. Select **Save**







Default Value:

Unset (disabled)

References:

1. <https://chromeenterprise.google/policies/#AutoOpenFileTypes>
2. <https://chromeenterprise.google/policies/#AutoOpenAllowedForURLs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

2.3.3.7.4 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Setting controls whether users can add exceptions to allow mixed content for specific sites.

- Do not allow any site to load mixed content
- Allow users to add exceptions to allow mixed content

The recommended state for this setting is: Do not allow any site to load mixed content

Rationale:

Allowing mixed (secure / insecure) content from a site can lead to malicious content being loaded. Mixed content occurs if the initial request is secure over HTTPS, but HTTPS and HTTP content is subsequently loaded to display the web page. HTTPS content is secure. HTTP content is insecure.

Impact:

Users will not be able to mix content.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Control use of insecure content exceptions**
7. Ensure **Control use of insecure content exceptions** is set to **Do not allow any site to load mixed content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Control use of insecure content exceptions**
7. Set **Control use of insecure content exceptions** to **Do not allow any site to load mixed content**
8. Select **Save**

Default Value:

Unset (Same as Enabled: Allow users to add exceptions to allow mixed content, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultInsecureContentSetting>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.7.5 (L1) Ensure 'Allow insecure content on these sites' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy specifies a list of pages that can display active mixed content, such as scripts and iframes. Also, Chrome does not automatically upgrade optionally-blockable, or passive, mixed content from HTTP to HTTPS. Passive mixed content includes images, audio, and video.

Rationale:

There needs to be no URLs in the configured settings.

Impact:

There should be no impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Control use of insecure content exceptions**
7. Ensure **Control use of insecure content exceptions** is not configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Allow insecure content on these sites**
7. Remove all URLs from **Allow insecure content on these sites**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#InsecureContentAllowedForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

2.3.3.7.6 (L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls whether websites are allowed to make requests to more private network endpoints in an insecure manner.

When this policy is set to true, all Private Network Access checks are disabled for all origins. This may allow attackers to perform CSRF attacks on private network servers.

Rationale:

This policy should not be configured.

Impact:

The only impact would be accessing insecure websites.

Audit:

To verify this setting via the Google Workspace Admin Console:




1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Requests from insecure websites to more-private network endpoints**
7. Ensure **Requests from insecure websites to more-private network endpoints** is not configured

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Requests from insecure websites to more-private network endpoints**
7. Remove all URLs from **Requests from insecure websites to more-private network endpoints**
8. Select **Save**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.3 <u>Deploy a Network Intrusion Detection Solution</u> Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.			
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

2.3.3.7.7 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome offers URL-keyed anonymized data collection as a feature. This sends URLs of pages the user visits to Google to optimize its services.

The recommended state for this setting is: **Disabled** (0)

Rationale:

Anonymized data collection shall be disabled, since it is unclear which specific information is sent to Google.

Impact:

Anonymized data will not be sent to Google to help optimize its services.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Enable URL-keyed anonymized data collection**
7. Ensure **Enable URL-keyed anonymized data collection** is set to **Data collection is never active**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Network**, select **Enable URL-keyed anonymized data collection**
7. Set **Enable URL-keyed anonymized data collection** to **Data collection is never active**
8. Select **Save**

Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#UrlKeyedAnonymizedDataCollectionEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.7.8 (L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting will allow specified URLs to access **file://** URLs in the PDF Viewer. By default all domains are blocked from accessing **file://** URLs in the PDF Viewer.

Rationale:

Blocking all domains, or a restricted list of domains, from opening a downloaded PDF file blocks the possibility of a malicious file being masked as a PDF. It could also block unknown or malicious code contained within the PDF that would run upon immediate opening within a browser tab.

Impact:

Users will be required to open PDF files manually in the PDF Viewer or in the organization's PDF viewing application.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **select Allow local file access to file:// URLs on these sites in the PDF Viewer**
7. Ensure **Allowed URLs** is empty

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Content**, select **Allow local file access to file:// URLs on these sites in the PDF Viewer**
7. Remove all URLs from **Allowed URLs**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PdfLocalFileAccessAllowedForDomains>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u> Train workforce members to be able to recognize a potential incident and be able to report such an incident.			
v7	3.3 <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.			

2.3.3.8 Power and shutdown

2.3.3.8.1 (L1) Ensure 'Idle settings' Is Configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

A locking screen saver is one of the standard security controls to limit access to a computer and the current user's session when the computer is temporarily unused or unattended.

Rationale:

Setting an inactivity interval for the screen saver prevents unauthorized persons from viewing a system left unattended for an extensive period of time.

Impact:

If the screen saver is not set, users may leave the computer available for an unauthorized person to access information.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Power and shutdown**, select **Idle settings**
7. Ensure **Idle settings** is set to your organization's requirements

Remediation:






To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Power and shutdown**, select **Idle settings**
7. Set **Idle settings** to your organization's requirements
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#ChromeOsLockOnIdleSuspend>
2. <https://chromeenterprise.google/policies/#IdleAction>
3. <https://chromeenterprise.google/policies/#IdleActionAC>
4. <https://chromeenterprise.google/policies/#IdleActionBattery>
5. <https://chromeenterprise.google/policies/#IdleDelayAC>
6. <https://chromeenterprise.google/policies/#IdleDelayBattery>
7. <https://chromeenterprise.google/policies/#IdleWarningDelayAC>
8. <https://chromeenterprise.google/policies/#IdleWarningDelayBattery>
9. <https://chromeenterprise.google/policies/#LidCloseAction>
10. <https://chromeenterprise.google/policies/#PowerManagementIdleSettings>
11. <https://chromeenterprise.google/policies/#PowerManagementUsesAudioActivity>
12. <https://chromeenterprise.google/policies/#PowerManagementUsesVideoActivity>
13. <https://chromeenterprise.google/policies/#ScreenDimDelayAC>
14. <https://chromeenterprise.google/policies/#ScreenDimDelayBattery>
15. <https://chromeenterprise.google/policies/#ScreenLockDelayAC>
16. <https://chromeenterprise.google/policies/#ScreenLockDelayBattery>
17. <https://chromeenterprise.google/policies/#ScreenLockDelays>
18. <https://chromeenterprise.google/policies/#ScreenOffDelayAC>
19. <https://chromeenterprise.google/policies/#ScreenOffDelayBattery>
20. <https://chromeenterprise.google/policies/#UserActivityScreenDimDelayScale>
21. <https://chromeenterprise.google/policies/#WaitForInitialUserActivity>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.1 Maintain an Inventory of Authentication Systems Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.			

2.3.3.9 Hardware

2.3.3.9.1 (L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome has an API which allows access to connected USB devices from the browser

- Do not allow any site to request access
- Allow sites to ask the user for access
- Allow the user to decide if sites can ask

The recommended state for this setting is Do not allow any site to request access.

Rationale:

WebUSB is opening the doors for sophisticated phishing attacks that could bypass hardware-based two-factor authentication devices (e.g. Yubikey devices).

Impact:

If this setting is configured, websites can no longer access connected USB devices via the API (this includes web cameras, headphones, and other USB devices) which could also prevent some two factor authentication (2FA) USB devices from working properly.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **WebUSB API**
7. Ensure **WebUSB API** is set to **Do not allow any site to request access**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **WebUSB API**
7. Set **WebUSB API** to **Do not allow any site to request access**
8. Select **Save**





Default Value:

Unset (Same as Enabled: Allow sites to ask the user for access, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultWebUsbGuardSetting>
2. <https://www.wired.com/story/chrome-yubikey-phishing-webusb/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

2.3.3.9.2 (L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting allows administrators to set whether the end-user is prompted for access to audio capture devices.

- **Disable audio input** - turns off prompts
- **Prompt user to allow each time** - users get prompted for audio capture access.

NOTE: The setting affects all audio input (not just the built-in microphone).

The recommended state for this setting is: **Disable audio input**

Rationale:

The end-user having the ability to allow or deny audio capture for websites in Google Chrome could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing audio capture, it removes the end-user's discretion, leaving it up to the organization which sites are allowed to use this ability.

Impact:

If you disable this setting, users will not be prompted for audio devices when using websites which may need this access, such as a web-based conferencing system. If there are sites to which access will be allowed, configuration of the *AudioCaptureAllowedUrls* setting will be necessary.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Audio input (microphone)**
7. Ensure **Audio input (microphone)** is set to **Disable audio input**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Audio input (microphone)**
7. Set **Audio input (microphone)** to **Disable audio input**
8. Select **Save**






Default Value:

Unset (Same as Prompt user to allow each time, but user can change)

References:

1. <https://chromeenterprise.google/policies/#AudioCaptureAllowed>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.3.9.3 (L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting allows administrators to set whether the end-user is prompted for access to video capture devices.

- **Disable camera input for websites and apps** - turns off prompts
- **Enable camera input for website and apps** - users get prompted for video capture access

NOTE: The setting affects all video input (not just the built-in camera).

The recommended state for this setting is **Disable camera input for websites and apps**.

Rationale:

The end-user having the ability to allow or deny video capture for websites in Google Chrome could open an organization up to a malicious site that may capture proprietary information through the browser. By limiting or disallowing video capture, it removes the end-user's discretion, leaving it up to the organization which sites are allowed to use this ability.

Impact:

If you disable this setting, users will not be prompted for video devices when using websites which may need this access, such as a web-based conferencing system. If there are sites to which access will be allowed, configuration of the `VideoCaptureAllowedUrls` setting will be necessary.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Video input (camera)**
7. Ensure **Configuration** is set to **Disable camera input for websites and apps**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Video input (camera)**
7. Set **Configuration** to **Disable camera input for websites and apps**
8. Select **Save**






Default Value:

Unset (Same as Enabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#VideoCaptureAllowed>
2. <https://chromeenterprise.google/policies/#VideoCaptureAllowedUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 <u>Use DNS Filtering Services</u> Use DNS filtering services on all enterprise assets to block access to known malicious domains.			
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

2.3.3.9.4 (L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls website access and use of the system serial port.

- Allow the user to decide (default) — Lets websites ask for access, but users can change this setting.
- Allow sites to ask the user to grant access to serial ports via the Web Serial API — Lets websites ask the user for access to serial ports.
- Do not allow any site to request access to serial ports via the Web Serial API

The recommended state for this setting is: **Do not allow any site to request access to serial ports via the Serial API**

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SerialAllowAllPortsForUrls*, *SerialAskForUrls* and *SerialBlockedForUrls* settings. For example, *SerialAllowAllPortsForUrls* can be used to allow serial port access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system serial ports may prevent malicious sites from using these ports and accessing the devices attached.

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Web Serial API**
7. Ensure **Web Serial API** is set to **Do not allow any site to request access to serial ports via the Web Serial API**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Web Serial API**
7. Set **Web Serial API** to **Do not allow any site to request access to serial ports via the Web Serial API**
8. Select **Save**





Default Value:

Unset (Same as Enabled with Allow sites to ask the user to grant access to a serial port, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSerialGuardSetting>
2. <https://chromeenterprise.google/policies/#SerialAskForUrls>
3. <https://chromeenterprise.google/policies/#SerialBlockedForUrls>
4. <https://chromeenterprise.google/policies/#SerialAllowAllPortsForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.3.9.5 (L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The privacy screen for ChromeOS is a feature that activates when the user walks away from the Chromebook. If activated, the screen will dim after 10 seconds. It can also keep the screen awake while the user is in front of the Chromebook even if they are not interacting with the device.

This policy requires a built in webcam and for ChromeOS devices with an integrated electronic privacy screen.

Rationale:

Setting the operating system to automatically dim and lock the screen when the user moves away from the device protects potentially sensitive user data.

Impact:

This should have no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Privacy screen**
7. Ensure **Privacy screen** is set to **Always enable the privacy screen**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Privacy screen**
7. Set **Privacy screen** to **Always enable the privacy screen**
8. Select **Save**

References:

1. <https://chromeenterprise.google/policies/#PrivacyScreenEnabled>
2. <https://support.google.com/chromebook/answer/12212810?hl=en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.9.6 (L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting controls website access and use of system sensors such as motion and light.

- Allow sites to access sensors
- Do not allow any site to access sensors

The recommended state for this setting is **Do not allow any site to access sensors**.

NOTE: If more granular control is needed (per website) then this setting can be used in combination with the *SensorsAllowedForUrls* and *SensorsBlockedForUrls* settings. For example, *SensorsAllowedForUrls* can be used to allow sensor access to specific sites. Please see the references below for more information.

Rationale:

Preventing access to system sensors may prevent malicious sites from using these sensors for user profiling (OpSec).

Impact:

This setting would also prevent legitimate sites from accessing it as well.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Sensors**
7. Ensure **Sensors** is set to **Do not allow any site to access sensors**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **Sensors**
7. Set **Sensors** to **Do not allow any site to access sensors**
8. Select **Save**

Default Value:

Unset (Same as Enabled with a value of Allow sites to access sensors, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DefaultSensorsSetting>
2. <https://chromeenterprise.google/policies/#SensorsAllowedForUrls>
3. <https://chromeenterprise.google/policies/#SensorsBlockedForUrls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.3.9.7 (L1) Ensure 'USB device detected notification' Is Set to 'Show notifications when USB devices are detected' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy controls notifications when USB devices are connected to a ChromeOS device. By default, notifications are shown when a USB device is connected. The settings are:

- **Show notifications when USB devices are detected** - notifications are shown when a USB device is connected
- **Do not show notifications when USB devices are detected** - notifications are not shown when a USB device is connected

Rationale:

A user should be alerted if a USB device is connected to their Google ChromeOS device. This allows the user to be notified if a device is connected without their knowledge or permission.

Impact:

None - this is the default.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **USB device detected notification**
7. Ensure **USB device detected notification** is set to **Show notifications when USB devices are detected**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Hardware**, select **USB device detected notification**
7. Set **USB device detected notification** to **Show notifications when USB devices are detected**
8. Select **Save**

Default Value:

Show notifications when USB devices are detected

References:

1. <https://chromeenterprise.google/policies/#UsbDetectorNotificationEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.3.10 Chrome Safe Browsing

2.3.3.10.1 (L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Control whether Google Chrome's Safe Browsing feature is enabled and the mode in which it operates. If you set this setting as mandatory, users cannot change or override the Safe Browsing setting in Google Chrome.

If this setting is left not set, Safe Browsing will operate in Standard Protection mode, but users can change this setting.

- Allow the user to decide
- Safe Browsing is never active
- Safe Browsing is active in the standard mode
- Safe Browsing is active in the enhanced mode. This mode provides better security, but requires sharing more browsing information with Google

The recommended state for this setting is: **Safe Browsing is active in the standard mode** or higher.

Rationale:

Google Safe Browsing will help protect users from a variety of malicious and fraudulent sites or from downloading dangerous files.

NOTE: Google recommends using Enhanced Safe Browsing Mode. Turning on Enhanced Safe Browsing will substantially increase protection from dangerous websites and downloads, but will share more data with Google.

For more details, please refer to the items in the References section below.

Impact:

There is no impact on the user.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Safe Browsing protection**
7. Ensure **Safe Browsing Protection Level** is set to **Safe Browsing is active in the standard mode**
8. Ensure **Allow Safe Browsing's standard protection mode to send partial hashes of URLs to Google** is set to **Allow higher-protection proxied lookups**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Safe Browsing protection**
7. Set **Safe Browsing Protection Level** to **Safe Browsing is active in the standard mode**
8. Set **Allow Safe Browsing's standard protection mode to send partial hashes of URLs to Google** to **Allow higher-protection proxied lookups**
9. Select **Save**





Default Value:

Unset (Same as Allow the user to decide, but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeBrowsingProtectionLevel>
2. <https://security.googleblog.com/2020/05/enhanced-safe-browsing-protection-now.html>
3. <https://security.googleblog.com/2021/06/new-protections-for-enhanced-safe.html>
4. https://developers.google.com/safe-browsing?_ga=2.65351149.274800631.1631808382-2031399475.1630502681

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.10.2 (L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google Chrome can block certain types of downloads, and won't let users bypass the security warnings, depending on the classification of Safe Browsing.

- No special restrictions (Default)
- Block malicious downloads
- Block malicious downloads and dangerous file types
- Block malicious downloads, uncommon or unwanted downloads and dangerous file types
- Block all downloads

The recommended state for this setting is **Block malicious downloads**.

NOTE: These restrictions apply to downloads triggered from webpage content, as well as the "Download link..." menu option. They don't apply to the download of the currently displayed page or to saving as PDF from the printing options.

Rationale:

Users shall be prevented from downloading malicious file types and shall not be able to bypass security warnings.

Impact:

If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings. These are downloads that have been identified as risky or from a risky source by the [Google Safe Browsing Global intelligence engine](#).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Download restrictions**
7. Ensure **Download restrictions** is set to **Block malicious downloads**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Download restrictions**
7. Set **Download restrictions** to **Block malicious downloads**
8. Select **Save**







Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DownloadRestrictions>
2. <https://developers.google.com/safe-browsing>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

2.3.3.10.3 (L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Google provides the Safe Browsing service. It shows a warning page when users navigate to sites that are flagged as potentially malicious. The settings for the policy are:

- Allow user to bypass Safe Browsing warning (Default)
- Do not allow user to bypass Safe Browsing warning

The recommended state for this setting is Do not allow user to bypass Safe Browsing warning.

Rationale:

Malicious web pages are widely spread on the internet and pose the most significant threat to the user today. Users shall be prevented from navigating to potentially malicious web content.

Impact:

Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. In some cases legitimate sites could be blocked and users would be prevented from accessing.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Disable bypassing Safe Browsing warnings**
7. Ensure **Disable bypassing Safe Browsing warnings** is set to **Do not allow user to bypass Safe Browsing warning**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Disable bypassing Safe Browsing warnings**
7. Set **Disable bypassing Safe Browsing warnings** to **Do not allow user to bypass Safe Browsing warning**
8. Select **Save**





Default Value:

Unset (Same as Allow user to bypass Safe Browsing warning, but user can change)

References:

1. <https://chromeenterprise.google/policies/#DisableSafeBrowsingProceedAnyway>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.10.4 (L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Google Chrome can use the Google Safe Search API to classify URLs as pornographic or not.

The recommended state for this setting is: **Filter top level sites (but not embedded iframes) for adult content**

Rationale:

Allowing search results to present sites that may have malicious content should be prohibited to help ensure users do not accidentally visit sites that are more prone to malicious content including spyware, adware, and viruses.

Impact:

Users' search results will be filtered and content such as adult text, videos, and images will not be shown.

NOTE: Using Google's Safe Search API may leak information which is typed/pasted by mistake into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **<https://admin.google.com>** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **SafeSites URL filter**
7. Ensure **SafeSites URL filter** is set to **Filter top level sites (but not embedded iframes) for adult content**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **SafeSites URL filter**
7. Set **SafeSites URL filter** to **Filter top level sites (but not embedded iframes)** for adult content
8. Select **Save**





Default Value:

Unset (Same as Enabled with "Do not filter sites for adult content", but user can change)

References:

1. <https://chromeenterprise.google/policies/#SafeSitesFilterBehavior>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.10.5 (L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting prevents the display of lookalike URL warnings on the sites listed. These warnings are typically shown on sites that Google Chrome believes might be trying to spoof another site with which the user is familiar.

Rationale:

Look-alike domains are intentionally misleading to give users the false impression that they're interacting with trusted brands, leading to significant reputation damage, financial losses, and data compromise for established enterprises.

In addition, this technique is commonly used to host phishing sites, and often leads to account takeover attacks. Users are prompted to enter their credentials on a fake website, and scammers take control of their online accounts with little effort to engage in fraudulent activity.

Impact:

None - This is the default behavior.

NOTE: The only real impact is possible user annoyance if they are going to a legitimate site that is falsely considered fraudulent (a rare occurrence). This can be handled by adding the site to the allowlist and/or notifying Google of the false finding.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select 'Suppress lookalike domain warnings'
7. Ensure **Allowlisted Domains** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Chrome Safe Browsing**, select **Suppress lookalike domain warnings on domains**
7. Remove all URLs from **Allowlisted Domains**
8. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#LookalikeWarningAllowlistDomains>
2. <https://safebrowsing.google.com/>
3. <https://bugs.chromium.org/p/chromium/issues/entry?template=Safety+Tips+Appeals>
4. <https://krebsonsecurity.com/2018/03/look-alike-domains-and-visual-confusion/>
5. <https://www.phishlabs.com/blog/the-anatomy-of-a-look-alike-domain-attack/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

2.3.3.11 Data Controls

2.3.3.11.1 (L2) Ensure 'Data controls reporting' Is Set to 'Enable reporting of data control events' (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy controls real-time reporting when the data leak prevention event triggers. This is disabled by default. Setting this policy to **Enable reporting of data leak prevention events** will switch on real-time reporting of data leak prevention events. Setting this policy to **Disable reporting of data leak prevention events** or leaving it unset will switch off the reporting.

Note: Data control rules are defined on the rules page which centralizes the creation and management of all rules. Please create and modify any Chrome action data control rules from there.

To access the rules page follow these instructions:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Rules**

Create rules based on your organization's requirements. Refer to the Google Enterprise Help Center for the [Set ChromeOS data controls documents](#).

Rationale:

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Data controls**, select **Data controls reporting**
7. Ensure **Data controls reporting** is set to **Enable reporting of data leak prevention events**
8. Select **Rules** in the left sidebar menu
9. Ensure **Rules** are set to your organization's requirements

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Settings**
5. Select **Managed guest session settings**
6. Under **Data controls**, select **Data controls reporting**
7. Set **Data controls reporting** to **Enable reporting of data leak prevention events**
8. Select **Save**
9. Select **Rules** in the left sidebar menu
10. Set **Rules** to your organization's requirements

Note: To set the appropriate rules for your organization, refer to the Google Enterprise Help Center for the [Set ChromeOS data controls documents](#).

References:

1. <https://support.google.com/chrome/a/answer/11587610>
2. <https://chromeenterprise.google/policies/#DataLeakPreventionReportingEnabled>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.4 Apps & extensions

2.4.1 (L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enabling this setting allows you to specify which app/extension types are allowed.

Disabled (0): Results in no restrictions on the acceptable extension and app types.

The recommended state for this setting is: **Enabled** with the values of **extension**, **hosted_app**, **platform_app**, **theme**.

Rationale:

App or extension types that could be misused or are deprecated shall no longer be installed.

NOTE: Google has removed support for Chrome Apps which includes the types **hosted_app** and **platform_app**. The blog post indicates that these types will require a setting to be enabled for continued use through June 2022.

Impact:

Extensions already installed will be removed if its type is denylisted and the extension itself is not allowlisted.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **Allowed types of apps and extensions**
7. Ensure **Configuration** is set to **Extension**, **Hosted App**, **Chrome Packaged App**, and **Theme**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **Allowed types of apps and extensions**
7. Set **Configuration** to **Extension, Hosted App, Chrome Packaged App, and Theme**
8. Select **Save**





Default Value:

Unset (Same as Disabled, but user can change)

References:

1. <https://chromeenterprise.google/policies/#ExtensionAllowedTypes>
2. <https://blog.chromium.org/2020/08/changes-to-chrome-app-support-timeline.html>
3. https://chromium.googlesource.com/chromium/src/+HEAD/extensions/docs/extension_and_app_types.md

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.4.2 (L1) Ensure 'App and extension install sources' Is Not Set (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blocklisted.

Disabled (0): then the user can install any extension in Google Chrome.

The recommended state for this setting is: **Enabled** with a value of *

NOTE: Chrome does offer a more granular permission-based configuration called **Extension management settings** if blocklisting all extensions is too aggressive, which allows an organization to drill down to the exact permissions that they want to lock down. The extensions management settings require more coordination and effort to understand what the security requirements are to block site and device permissions globally, as well as more IT management to deploy. The benefit would be allowing access to more extensions to their end-users. See link in reference section.

NOTE: If Chrome Cleanup is Disabled, users may want to configure the extension blocklist instead of using the Extension Management option. Chrome Cleanup can help protect against malicious extensions when paired with the Extension Management setting.

Rationale:

This can be used to block extensions that could potentially allow remote control of the system through the browser. If there are extensions needed for securing the browser or for enterprise use, these can be enabled by configuring either the setting **Configure extension installation allowlist** or the setting **Extension management settings**.

Impact:

Any installed extension will be removed unless it is specified on the extension allowlist. If an organization is using any approved password managers, ensure that the extension is added to the allowlist.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Under **User & browser settings**, select **Additional Settings**
6. Ensure **App and extension install sources** is empty

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **App and extension install sources**
7. Ensure **Configuration** is empty

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **App and extension install sources**
7. Remove all URLs from **Configuration**
8. Select **Save**





Default Value:

Unset (Same as Disabled, and users can change)

References:

1. <https://chromeenterprise.google/policies/#ExtensionInstallBlocklist>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	<u>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

2.4.3 (L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy disables any extensions in Google Chrome that were downloaded from the Chrome Web Store and are now unpublished. The policy can be configured to either:

- Enabled (0): **Allow unpublished extensions**
- Disabled (1): **Disable unpublished extensions**

If the value for **ExtensionUnpublishedAvailability** is not changed from the default, it will behave as if it is enabled.

Note: Off-store extensions such as unpacked extensions installed using developer mode and extensions installed using the command-line switch are ignored. Force-installed extensions that are self-hosted are ignored. All version-pinned extensions are also ignored.

Rationale:

Disabling unpublished extensions will remove the ability to run any extensions that are no longer being updated or patched.

Impact:

This may disable extensions commonly used by users in your organization.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to **https://admin.google.com** as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **Chrome Web Store unpublished extensions**
7. Ensure **Configuration** is set to **Disable unpublished extensions**

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Devices**
3. Select **Chrome**
4. Select **Apps & extensions**
5. Select **User app settings**
6. Under **Additional app settings**, select **Chrome Web Store unpublished extensions**
7. Set **Configuration** to **Disable unpublished extensions**
8. Select **Save**







Default Value:

Allow unpublished extensions

References:

1. <https://chromeenterprise.google/policies/#ExtensionUnpublishedAvailability>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.2 <u>Establish and Maintain a Remediation Process</u> Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

3 Apps

3.1 Google Workspace

The Google Workspace sub-section of the Google Workspace Admin Console.

3.1.1 Gmail

Gmail settings.

3.1.1.1 User Settings

Set name formats. Enable user preferences such as themes, read receipts, and email delegation.

3.1.1.1.1 (L1) *Ensure users cannot delegate access to their mailbox (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Mail delegation allows the delegate to read, send, and delete messages on their behalf. For example, a manager can delegate Gmail access to another person in their organization, such as an administrative assistant.

Rationale:

Only administrators should be able to delegate access to a user's mailboxes.

Impact:

Existing delegations will be hidden when this feature is disabled.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **User Settings - Mail delegation**, ensure **Let users delegate access to their mailbox to other users in the domain** is **unchecked**

Remediation:







To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **User Settings - Mail delegation**, set **Let users delegate access to their mailbox to other users in the domain** to **unchecked**
6. Select **Save**

Default Value:

Let users delegate access to their mailbox to other users in the domain is **unchecked**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.1.1.2 Safety

Configure email and spam safety features.

3.1.1.2.1 Attachments

Additional policies to protect against malware in emails.

3.1.1.2.1.1 (L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an encrypted attachment from an untrusted sender.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, ensure **Protect against encrypted attachments from untrusted senders** is checked

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, set **Protect against encrypted attachments from untrusted senders** to checked
6. Select **Save**

Default Value:

Protect against encrypted attachments from untrusted senders is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 <u>Block Unnecessary File Types</u> Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	7.9 <u>Block Unnecessary File Types</u> Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.			

3.1.1.2.1.2 (L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an attachment with scripts from an untrusted sender.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, ensure **Protect against attachments with scripts from untrusted senders** is checked

Remediation:





To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, set **Protect against attachments with scripts from untrusted senders** to checked
6. Select **Save**

Default Value:

Protect against attachments with scripts from untrusted senders is enabled is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	7.9 Block Unnecessary File Types Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.			

3.1.1.2.1.3 (L1) *Ensure protection against anomalous attachment types in emails is enabled (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an anomalous attachment.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, ensure **Protect against anomalous attachment types in emails** is checked

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Attachments**, set **Protect against anomalous attachment types in emails** to checked
6. Select **Save**

Default Value:

Protect against anomalous attachment types in emails is Unchecked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 <u>Block Unnecessary File Types</u> Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	7.9 <u>Block Unnecessary File Types</u> Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.			

3.1.1.2.2 Links and external images

Additional settings to prevent email phishing due to links and external images.

3.1.1.2.2.1 (L1) Ensure link identification behind shortened URLs is enabled (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Identify links behind short URLs, and display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, ensure **Identify links behind shortened URLs** is checked

Remediation:





To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, set **Identify links behind shortened URLs** to checked
6. Select **Save**

Default Value:

Identify links behind shortened URLs is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

3.1.1.2.2.2 (L1) Ensure scan linked images for malicious content is enabled (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Scan linked images for malicious content, and display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, ensure **Scan linked images** is **checked**

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, set **Scan linked images** to **checked**
6. Select **Save**

Default Value:

Scan linked images is **checked**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 <u>Block Unnecessary File Types</u> Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	7.9 <u>Block Unnecessary File Types</u> Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.			

3.1.1.2.2.3 (L1) *Ensure warning prompt is shown for any click on links to untrusted domains (Manual)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, ensure **Show warning prompt for any click on links to untrusted domains** is checked

Remediation:





To configure this setting via the Google Workspace Admin Console:

1. Log in to <https://admin.google.com> as an administrator
2. Select **Apps**
3. Select **Google Workspace**
4. Select **Gmail**
5. Under **Safety - Links and external images**, set **Show warning prompt for any click on links to untrusted domains** is checked
6. Select **Save**

Default Value:

Show warning prompt for any click on links to untrusted domains is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

4 Rules

The **Rules** section of Google Workspace is where your organization can set data control rules. There is no specific guidance around what rules your organization should create, but there should be rules based on what your security team has decided to monitor. Refer to the Google Enterprise Help Center for the [Set ChromeOS data controls documents](#).

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Directory		
1.1	Users		
1.1.1	(L1) Ensure more than one Super Admin account exists (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	Chrome		
2.1	Devices		
2.1.1	(L1) Review Devices Periodically (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Enrollment tokens		
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Settings		
2.3.1	User & Browser		
2.3.1.1	General		
2.3.1.1.1	(L1) Ensure 'Maximum user session length' Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1.2	(L1) Ensure 'Custom terms of service' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2	Apps and extensions		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3	Site isolation		
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4	Security		
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.3	(L1) Ensure 'Online revocation checks' is set to 'Do not perform online OCSP/CRL checks' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.4	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.5	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.6	(L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.7	(L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.4.8	(L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.9	(L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.11	(L2) Ensure 'Online revocation checks' is set to 'Perform online OCSP/CRL checks' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.12	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.13	(L1) Ensure 'Google online login frequency' Is Set to '1' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.14	(L1) Ensure 'Google online unlock frequency' is set to '1' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.15	(L1) Ensure 'SAML single sign-on login frequency is set to 'Every day' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.16	(L1) Ensure 'SAML single sign-on unlock frequency is set to '1' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.17	(L1) Ensure 'Allowed certificate transparency URLs' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.18	(L1) Ensure 'Certificate transparency CA allowlist' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.19	(L1) Ensure 'Certificate transparency legacy CA allowlist' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.20	(L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.4.21	(L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.24	(L2) Ensure Advanced Protection Program is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.25	(L1) Ensure 'Override insecure origin restrictions' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.26	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.27	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.28	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.30	(L1) Ensure 'Media picker without user gesture' Is Not Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5	Remote Access		
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.6	Session Settings		
2.3.1.6.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7	Network		
2.3.1.7.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.3	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.4	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.7	(L1) Ensure 'Cross-origin authentication' is set to 'Block cross-origin authentication' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.8	(L1) Ensure 'Enable globally scoped HTTP authentication cache' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.9	(L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.10	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks ' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.7.11	(L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8	Content		
2.3.1.8.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.2	(L2) Ensure 'Screen video capture' is set to 'Do not allow sites to prompt the user to share a video stream of their screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.3	(L2) Ensure 'Cookies' is set to 'Session Only' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.5	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.7	(L2) Ensure 'Notifications' is set to 'Do not allow any site to show desktop notifications' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.9	(L1) Ensure 'Cast' is set to 'Do not allow users to cast' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.10	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.8.11	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.12	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9	User experience		
2.3.1.9.1	(L1) Ensure 'Download location prompt' is set to 'Ask the user where to save the file before downloading' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.8	(L1) Ensure 'Network prediction' Is Set to 'Do not predict network actions' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.10	(L2) Ensure 'Native Messaging blocked hosts' is set to '*' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.12	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.10	Connected devices		
2.3.1.11	Omnibox Search Provider		
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12	Hardware		
2.3.1.12.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.12.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.7	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.13	User verification		
2.3.1.13.1	(L2) Ensure 'Verified Mode' Is Set to 'Require verified mode boot for Verified Access' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14	Browser Reporting		
2.3.1.14.1	(L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.2	(L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15	Chrome Safe Browsing		
2.3.1.15.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.2	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.5	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.15.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.7	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.8	(L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16	Generative AI		
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17	Chrome updates		
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18	Chrome variations		
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19	Other settings		
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19.2	(L1) Ensure 'Chrome Sync (ChromeOS)' is set to 'Allow Chrome Sync' and Exclude 'Passwords' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Device Settings		
2.3.2.1	Enrollment and access		
2.3.2.1.1	(L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.3	(L2) Ensure 'Verified access' Is Set to 'Enable for content protection' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.4	Ensure 'Disabled device return instructions' Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Sign-in settings		
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.2.2.3	(L2) Ensure 'Sign-in screen' Is Set to 'Never show user names and photos' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.4	(L1) Ensure 'User data' Is Set to 'Do not erase local user data' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.5	(L1) Ensure 'Privacy screen on sign-in screen' Is Set to 'Always enable the privacy screen on sign-in screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.6	(L1) Ensure 'Show numeric keyboard for password' Is Set to 'Default to a standard keyboard for password input' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3	Device update settings		
2.3.2.3.1	Auto-update settings		
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.3	(L2) Ensure 'Roll back to target version' Is Set to 'Do not roll back OS' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.4	(L1) Ensure 'Release channel' Is Set to 'Stable channel' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.6	(L2) Ensure 'Peer to peer' Is Set to 'Do not allow peer to peer auto update downloads' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.8	Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.2	(L1) Ensure 'Variations' Is Set to 'Enable Chrome variations' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.2.4	User and device reporting		
2.3.2.4.1	(L1) Ensure 'Metrics reporting' Is Set to 'Never send metrics to Google' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5	Other settings		
2.3.2.5.1	(L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.2	(L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.6	Security		
2.3.2.6.1	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Managed guest session settings		
2.3.3.1	General		
2.3.3.1.1	(L1) Ensure 'Managed guest session' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.2	(L1) Ensure 'Maximum user session length' Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.3	(L1) Ensure 'Custom terms of service' Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2	Apps and extensions		
2.3.3.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Security		
2.3.3.3.1	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.2	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.4	(L2) Ensure 'Incognito mode' is set to 'Disallow incognito mode' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.5	(L1) Ensure 'Browser history' is set to 'Always save browser history' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.6	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.9	(L1) Ensure 'Media picker without user gesture' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4	Remote access		
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.4.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.5	Session settings		
2.3.3.5.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6	Network		
2.3.3.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.4	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.5	(L1) Ensure 'SharedArrayBuffer' Is Set to 'Prevent sites that are not cross-origin isolated from using SharedArrayBuffers' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.6	(L1) Ensure 'Globally scoped HTTP authentication cache' is set to 'HTTP authentication credentials are scoped to top-level sites' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.7	(L1) Ensure 'HSTS policy bypass list' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.8	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.7	Content		
2.3.3.7.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.2	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.4	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.6	(L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.7	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8	Power and shutdown		
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9	Hardware		
2.3.3.9.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.7	(L1) Ensure 'USB device detected notification' Is Set to 'Show notifications when USB devices are detected' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10	Chrome Safe Browsing		
2.3.3.10.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.4	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.11	Data Controls		
2.3.3.11.1	(L2) Ensure 'Data controls reporting' Is Set to 'Enable reporting of data control events' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4	Apps & extensions		
2.4.1	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'App and extension install sources' Is Not Set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Apps		
3.1	Google Workspace		
3.1.1	Gmail		
3.1.1.1	User Settings		
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2	Safety		
3.1.1.2.1	Attachments		
3.1.1.2.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2	Links and external images		
3.1.1.2.2.1	(L1) Ensure link identification behind shortened URLs is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.1.2.2.2	(L1) Ensure scan linked images for malicious content is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4	Rules		

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.9	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.11	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.1	(L1) Ensure 'Managed guest session' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1.1	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.5	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.9	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.12	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.24	(L2) Ensure Advanced Protection Program is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.27	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.3	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.4	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.9	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.10	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.9	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.10	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.8.11	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.12	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.10	(L2) Ensure 'Native Messaging blocked hosts' is set to '*'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.12.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.7	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.13.1	(L2) Ensure 'Verified Mode' Is Set to 'Require verified mode boot for Verified Access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.1	(L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.2	(L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.2	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.5	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.7	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.8	(L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.1	(L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.3	(L2) Ensure 'Verified access' Is Set to 'Enable for content protection'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.6	(L2) Ensure 'Peer to peer' Is Set to 'Do not allow peer to peer auto update downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.8	Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.6.1	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.1	(L1) Ensure 'Managed guest session' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.2	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.1	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.2	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.6	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.6.4	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.7	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.8	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.4	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.10.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'App and extension install sources' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.1	(L1) Ensure link identification behind shortened URLs is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.2	(L1) Ensure scan linked images for malicious content is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1.1	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.5	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.9	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.12	(L1) Ensure 'Geolocation' is set to 'Do not allow sites to detect users' geolocation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.24	(L2) Ensure Advanced Protection Program is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.26	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.27	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.28	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.3	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.4	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.9	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.10	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.11	(L1) Ensure 'Http Allowlist' Is Properly Configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.9	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.10	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.11	(L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Data collection is never active'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.12	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.9.10	(L2) Ensure 'Native Messaging blocked hosts' is set to '*'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.12	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.7	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.13.1	(L2) Ensure 'Verified Mode' Is Set to 'Require verified mode boot for Verified Access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.1	(L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.2	(L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.2	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.5	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.7	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.8	(L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.1.1	(L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.3	(L2) Ensure 'Verified access' Is Set to 'Enable for content protection'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.6	(L2) Ensure 'Peer to peer' Is Set to 'Do not allow peer to peer auto update downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.8	Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.1	(L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.2	(L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.6.1	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.1	(L1) Ensure 'Managed guest session' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.2	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.1	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.3.2	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.5	(L1) Ensure 'Browser history' is set to 'Always save browser history'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.6	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.4	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.7	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.8	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.6	(L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.4	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'App and extension install sources' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.1	(L1) Ensure link identification behind shortened URLs is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.2	(L1) Ensure scan linked images for malicious content is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.4	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.6	(L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.7	(L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.13	(L1) Ensure 'Google online login frequency' Is Set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.14	(L1) Ensure 'Google online unlock frequency' is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.15	(L1) Ensure 'SAML single sign-on login frequency is set to 'Every day'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.16	(L1) Ensure 'SAML single sign-on unlock frequency is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.4.20	(L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.21	(L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.26	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.6.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.5	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.4	(L1) Ensure 'User data' Is Set to 'Do not erase local user data'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.5.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1.1	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.4	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.5	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.6	(L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.7	(L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.13	(L1) Ensure 'Google online login frequency' Is Set to '1'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.4.14	(L1) Ensure 'Google online unlock frequency' is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.15	(L1) Ensure 'SAML single sign-on login frequency is set to 'Every day'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.16	(L1) Ensure 'SAML single sign-on unlock frequency is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.20	(L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.21	(L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.24	(L2) Ensure Advanced Protection Program is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.26	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.27	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.6.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.7.3	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.4	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.9	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.10	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.5	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.9	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.10	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.12	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.10	(L2) Ensure 'Native Messaging blocked hosts' is set to '*'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.7	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.14.1	(L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.2	(L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.2	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.5	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.7	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.8	(L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.1	(L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.3	(L2) Ensure 'Verified access' Is Set to 'Enable for content protection'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.4	(L1) Ensure 'User data' Is Set to 'Do not erase local user data'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.1	(L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.2	(L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.6.1	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.2	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.1	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.2	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.6	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.5.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.4	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.7	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.6.8	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.6	(L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.4	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.4.1	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'App and extension install sources' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.1	(L1) Ensure link identification behind shortened URLs is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.2	(L1) Ensure scan linked images for malicious content is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure Super Admin accounts are used only for Super Admin activities	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	(L1) Review Devices Periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(L1) Ensure Any Unused Enrollment Tokens Are Revoked	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1.1	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.1	(L1) Ensure 'Task Manager' Is Set to 'Block users from ending processes with the Chrome task manager'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3.1	(L1) Ensure 'Site isolation' is set to 'Require Site Isolation for all websites, as well as any origins below'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.1	(L1) Ensure 'Password manager' is Explicitly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.2	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.4	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.5	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.6	(L1) Ensure 'Lock screen PIN' Is Set to 'Do not allow users to set a weak PIN' and a minimum PIN length of 6 or greater	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.7	(L1) Ensure 'PIN auto-submit' Is Set to 'Disable PIN auto-submit on the lock and login screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.10	(L1) Ensure 'Clear browser history' Is Set to 'Do not allow clearing history in settings menu'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.13	(L1) Ensure 'Google online login frequency' Is Set to '1'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.4.14	(L1) Ensure 'Google online unlock frequency' is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.15	(L1) Ensure 'SAML single sign-on login frequency is set to 'Every day'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.16	(L1) Ensure 'SAML single sign-on unlock frequency is set to '1'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.20	(L1) Ensure 'User management of installed CA certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.21	(L1) Ensure 'User management of installed client certificates' Is Set to 'Disallow users from managing certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.22	(L1) Ensure 'Enable leak detection for entered credentials' Is Set to 'Enable Leak detection for entered credentials'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.23	(L1) Ensure 'Unsupported system warning' is set to 'Allow Chrome to display warnings when running on an unsupported system'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.24	(L2) Ensure Advanced Protection Program is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.26	(L1) Ensure 'Allow remote debugging' is set to 'Do not allow use of the remote debugging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.27	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.28	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4.29	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.1	(L2) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.6.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.7.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.3	(L2) Ensure 'Supported authentication schemes' is set to 'NTLM' and 'Negotiate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.4	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.5	(L1) Ensure 'WebRTC ICE candidate URLs for local IPs' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.6	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.9	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.10	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks '	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.11	(L1) Ensure 'Http Allowlist' Is Properly Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.7.12	(L1) Ensure 'Automatic HTTPS upgrades' Is Set to 'Allow HTTPS upgrades'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.4	(L1) Ensure 'Third-party cookie blocking' is set to 'Disallow third-party cookies'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.5	(L1) Ensure 'First-Party Sets' Is Set to 'Disable First-Party Sets for all affected users'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.6	(L1) Ensure 'Clipboard' Is Set to 'Do not allow any site to use the clipboard site permission'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.8	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.9	(L1) Ensure 'Cast' is set to 'Do not allow users to cast'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.10	(L1) Ensure 'Control use of insecure content exceptions' is set to 'Do not allow any site to load mixed content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.12	(L2) Ensure 'Web Bluetooth API' is set to 'Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.8.13	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.8.14	(L2) Ensure 'Third-party storage partitioning' Is Set to 'Block third-party storage partitioning from being enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.2	(L1) Ensure 'Spell check service' is set to 'Disable the spell checking web service'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.3	(L2) Ensure 'Google Translate' is set to 'Never offer translation'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.4	(L1) Ensure 'Alternate error pages' is set to 'Never use alternate error pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.5	(L2) Ensure 'Address form Autofill' is set to 'Never Autofill address forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.6	(L1) Ensure 'Credit card form Autofill' is set to 'Never Autofill credit card forms'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.7	(L1) Ensure 'Payment methods' is set to 'Always tell websites that no payment methods are saved'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.9	(L2) Ensure 'Browser guest mode' is set to 'Prevent guest browser logins'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.10	(L2) Ensure 'Native Messaging blocked hosts' is set to '*'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.11	(L1) Ensure 'Allow user feedback' is set to 'Do not allow user feedback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.9.12	(L2) Ensure 'File selection dialogs' is set to 'Block file selection dialogs'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.1	(L2) Ensure 'Search suggest' is set to 'Never allow users to use Search Suggest'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.11.2	(L1) Ensure 'Side Panel search' Is Set to 'Disable Side Panel search on all web pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access to USB devices via the WebUSB API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.5	(L1) Ensure 'Privacy screen' Is Set to 'Always enable the privacy screen'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.12.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.12.7	(L1) Ensure 'Enterprise Hardware Platform API' is set to 'Do not allow managed extensions to use the Enterprise Hardware Platform API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.1	(L1) Ensure 'Managed browser reporting' Is Set to 'Enable managed browser cloud reporting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.14.2	(L1) Ensure 'Managed browser reporting upload frequency' Is Set to Less Than or Equal to 24 Hours	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode', 'Allow real time proxied checks', and 'Do not allow users to override this setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.2	(L1) Ensure no URLs Are Configured in 'Safe Browsing allowed domains'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.3	(L1) Ensure 'Safe Browsing for trusted sources' is set to 'Perform Safe Browsing checks on all downloaded files'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.4	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.5	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.6	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.7	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.15.8	(L1) Ensure 'Abusive Experience Intervention' is set to 'Prevent sites with abusive experiences from opening new windows or tabs'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.1	Ensure 'Generative AI policy defaults' Is Set to 'Allow GenAI features without improving AI models'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.2	Ensure 'Help me write' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.3	Ensure 'DevTools AI features' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.4	Ensure 'History search settings' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.16.5	Ensure 'Tab compare' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.16.6	Ensure 'Help me read' Is Set to 'Use the value specified in the Generative AI policy defaults setting'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.1	(L1) Ensure 'Component updates' is set to 'Enable updates for all components'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.2	(L1) Ensure 'Relaunch notification' sets 'Time Period (hours)' to '168 or less' and 'Initial quiet period (hours)' to less than 'Time Period (hours)'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.17.3	(L1) Ensure 'Relaunch notification' is set to 'Show notification recommending relaunch'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.18.1	(L1) Ensure 'Variations' is set to 'Enable Chrome variations'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.19.1	(L1) Ensure 'Allow reporting of domain reliability related data' Is 'Never send domain reliability data to Google'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.1	(L1) Ensure 'Forced re-enrollment' Is Set to 'Force device to re-enroll with user credentials after wiping'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.2	(L1) Ensure 'Powerwash' Is Set to 'Allow powerwash to be triggered'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1.3	(L2) Ensure 'Verified access' Is Set to 'Enable for content protection'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.1	(L1) Ensure 'Guest mode' Is Set to 'Disable guest mode'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.2	(L1) Ensure 'Sign-in restriction' Is Set to 'Restrict sign-in to a list of users' and Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2.4	(L1) Ensure 'User data' Is Set to 'Do not erase local user data'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.1	(L1) Ensure 'Allow devices to automatically update OS version' Is Set to 'Allow updates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.2	(L1) Ensure 'Target version' Is Set to Either 'Use latest version' or no older than n-3	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.5	(L1) Ensure 'Rollout plan' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.7	(L2) Ensure 'Enforce updates' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.3.1.8	Ensure 'Update downloads' Is Set to 'Use HTTPS for update downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.4.2	(L1) Ensure 'Device system log upload' Is Set to 'Enable device system log upload'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.5.1	(L2) Ensure 'Authenticated Proxy Traffic' Is Set to 'Block system traffic to go through a proxy with authentication'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.5.2	(L1) Ensure 'Enable Key Locker' Is Set to 'Use Key Locker with the encryption algorithm for user storage encryption'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.6.1	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.1	(L1) Ensure 'Managed guest session' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1.2	(L1) Ensure 'Maximum user session length' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2.2	(L2) Ensure 'Manifest v2 extension availability' Is Set to 'Enable force-installed manifest v2 extensions on the sign-in screen'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.1	(L1) Ensure 'Web Authentication requests on sites with broken TLS certificates' Is Set to 'Do not allow WebAuthn API requests on sites with broken TLS certificates'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.2	(L1) Ensure 'Insecure hashes in TLS handshakes' Is Set to 'Do not allow insecure hashes in TLS handshakes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.3	(L1) Ensure 'Post-quantum TLS' Is Set to 'Allow post-quantum key agreement in TLS connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.6	(L1) Ensure 'TLS encrypted ClientHello' Is 'Enable the TLS Encrypted ClientHello experiment'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.7	(L1) Ensure 'Strict MIME type checking for worker scripts' Is Set to 'Require a JavaScript MIME type for worker scripts'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3.8	(L1) Ensure 'File/directory picker without user gesture' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.1	(L1) Ensure 'Remote access clients' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.2	(L1) Ensure 'Remote access hosts' is set with a domain defined in 'Remote access host domain'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.3	(L1) Ensure 'Firewall traversal' is set to 'Disable the use of relay servers'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.4.4	(L1) Ensure 'Remote support connections' is set to 'Prevent remote support connections'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.5.1	(L1) Ensure 'Show sign-out button in tray' Is Set to 'Show sign-out button in tray'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.6.1	(L1) Ensure 'Proxy mode' is Not Set to 'Always auto detect the proxy'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.2	(L2) Ensure 'Ignore proxy on captive portals' Is Set to 'Keep policies for captive portal pages'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.3	(L2) Ensure 'SSL error override' is set to 'Block users from clicking through SSL warnings'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.4	(L2) Ensure 'DNS over HTTPS' is set to 'Enable DNS-over-HTTPS without insecure fallback'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.7	(L1) Ensure 'HSTS policy bypass list' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.6.8	(L1) Ensure 'DNS interception checks enabled' is set to 'Perform DNS interception checks'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.1	(L2) Ensure 'SafeSearch and Restricted Mode' is set to 'Always use Safe Search for Google Web Search queries'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.3	(L1) Ensure 'Auto open downloaded files' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.5	(L1) Ensure 'Allow insecure content on these sites' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.6	(L2) Ensure 'Requests from insecure websites to more-private network endpoints' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.7.8	(L1) Ensure 'Local file access to file:// URLs on these sites in the PDF Viewer' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.8.1	(L1) Ensure 'Idle settings' Is Configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.1	(L2) Ensure 'WebUSB API' is set to 'Do not allow any site to request access'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.2	(L2) Ensure 'Audio input (microphone)' is set to 'Disable audio input'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.3	(L2) Ensure 'Video input (camera)' is set to 'Disable camera input for websites and apps'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.4	(L2) Ensure 'Web Serial API' is set to 'Do not allow any site to request access to serial ports via the Web Serial API'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.9.6	(L2) Ensure 'Sensors' is set to 'Do not allow any site to access sensors'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.1	(L1) Ensure 'Safe Browsing protection' is set to 'Safe Browsing is active in the standard mode' and 'Allow higher-protection proxied lookups'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.3.10.2	(L1) Ensure 'Download restrictions' is set to 'Block malicious downloads'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.3	(L1) Ensure 'Disable bypassing Safe Browsing warnings' is set to 'Do not allow user to bypass Safe Browsing warning'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.4	(L2) Ensure 'SafeSites URL filter' is set to 'Filter top level sites (but not embedded iframes) for adult content'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.10.5	(L1) Ensure 'Suppress lookalike domain warnings on domains' is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	(L1) Ensure 'Allowed types of apps and extensions' is set to 'Extension', 'Hosted App', 'Chrome Packaged App', and 'Theme'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'App and extension install sources' Is Not Set	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Chrome Web Store unpublished extensions' Is Set to 'Disable unpublished extensions'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.1.1	(L1) Ensure users cannot delegate access to their mailbox	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.1	(L1) Ensure link identification behind shortened URLs is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.2	(L1) Ensure scan linked images for malicious content is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Aug 29, 2025	1.1.0	Create recommendation for Post-quantum TLS for Device Settings and Managed Guest Session Settings (Ticket 25638)
Aug 29, 2025	1.1.0	Update rationale to include what data Google collects and add support document link (Ticket 24926)
Aug 29, 2025	1.1.0	Import Media Picker without user gesture from Chrome Core (Ticket 25616)
Aug 29, 2025	1.1.0	Import Enable Leak Detection Recommendation from Chrome Core (Ticket 25615)
Aug 29, 2025	1.1.0	Should there be recommendations created for: Passkeys, Account Recovery, Quick Unlock, WebAuthn, Lock Screen PIN, Google online and SAML sign-on options, URLs allowed for multi-screen capture (Ticket 25617)
Aug 29, 2025	1.1.0	Import Post-quantum TLS from Chrome benchmark (Ticket 25612)
Aug 29, 2025	1.1.0	Update login frequency to 1 instead of 0 (Ticket 25670)

Date	Version	Changes for this version
Aug 29, 2025	1.1.0	Add 'Abusive Experience Intervention' recommendation (Ticket 25663)
Aug 29, 2025	1.1.0	Create Help Me Read Recommendation (Ticket 25637)
Aug 29, 2025	1.1.0	Should either AI Feature intro or Gemini intro during sign-in as recommendations (Ticket 25611)
Aug 29, 2025	1.1.0	Update 'Chrome Web Store unpublished extensions' to reflect new location and settings (Ticket 25669)
Aug 29, 2025	1.1.0	Update 'App and extension install sources' to reflect new location and settings (Ticket 25668)
Aug 29, 2025	1.1.0	Update 'Allowed types of apps and extensions' to reflect new location and settings (Ticket 25667)
Aug 29, 2025	1.1.0	Reorder Hardware sub-section to mirror Workspace GUI (Ticket 25666)
Aug 29, 2025	1.1.0	Rearrange Network sub-section to mirror Workspace GUI (Ticket 25665)
Aug 29, 2025	1.1.0	Update title to Device Settings from just Device (Ticket 25664)
Aug 29, 2025	1.1.0	Configuration is not available as per CIS (Ticket 24971)

Date	Version	Changes for this version
Aug 29, 2025	1.1.0	Import Generative AI Sub-section and recommendations from Chrome Core (Ticket 25636)
Aug 29, 2025	1.1.0	Re-ordered Chrome Safe Browsing Section to Mirror Workspace GUI (Ticket 25635)
Aug 29, 2025	1.1.0	Reorder Hardware sub-section to mirror Workspace GUI (Ticket 25662)
Aug 29, 2025	1.1.0	WebUSB API recommendation was incorrectly located in the Content sub-section and is moved to Hardware sub-section (Ticket 25661)
Aug 29, 2025	1.1.0	Re-ordered User Experience Section to Mirror Workspace GUI (Ticket 25632)
Aug 29, 2025	1.1.0	Re-ordered Content Section to Mirror Workspace GUI (Ticket 25629)
Aug 29, 2025	1.1.0	Reorder recommendations to mirror Workspace GUI (Ticket 25619)
Aug 29, 2025	1.1.0	Re-ordered Security Section to Mirror Workspace GUI (Ticket 25614)
Aug 29, 2025	1.1.0	Should recommendations be added for: Ignore proxy on captive portals (Ticket 25620)

Date	Version	Changes for this version
Aug 29, 2025	1.1.0	Duplicate recommendation (Ticket 25628)
Aug 29, 2025	1.1.0	Update title to match Workspace GUI - Native Messaging blocked hosts (Ticket 25660)
Aug 29, 2025	1.1.0	Allow third-party partitioning to be enabled is deprecated and needs to be removed (Ticket 25659)
Aug 29, 2025	1.1.0	Delete duplicate recommendation (Ticket 25658)
Aug 29, 2025	1.1.0	Remove Enforce local anchor constraints due to deprecation (Ticket 25646)