Original console

Policies

1. Android

◎ : Supported on Work Profile on Company-Owned devices

Policies	Feature	Android Enterprise		Android Enterprise - Android Management API		Samsung Knox	
		Device controls	Work profile controls	Device controls	Work profile controls	Device controls	Work profile controls
System	Set user certificates	○	◎	○	○	○	◎
	Use camera	◎	◎	◎	◎	◎	◎
	Screen capture permission	◎	◎	◎	◎	◎	◎
	Block use of certain hardware keys	◎					
	Use VPN	○	◎	○	◎	○	◎
	Add or Delete account (+Account type blocklist/allowlist)	◎	◎	◎	◎	◎	◎
	Allow changes to Managed Google Play	◎	◎			◎	◎
	Install system updates	◎		◎		◎	
	Developer mode	○		◎		◎	
	User deletion	○				○	
	Safe mode	◎				◎	
	Change wallpaper	○				○	
	Set custom wallpaper	○				○	
	Factory reset	○				○	
	Transfer data using NFC	○		◎			
	Show overlay pop-ups and alerts	○				○	
	Android easter egg game	○				○	
	Change brightness setting	○				○	
	Always on display	○				○	
	Show error notification after app crash	○				○	
	Take action if OS is compromised	○				○	
	Show notification if event is triggered	○				○	
	Show notification if event is disabled	○				○	
	Remove notifications from quick panel	○					
	Set encryption for device storage	○				○	
	Set date and time	◎		◎		○	
	Change language	○				○	
	Backup data on cloud	○				○	
	Show message for blocked settings	○				○	
	Show custom message on lock screen	○		◎		○	
	Mount physical media			◎			
	Domain blocklist settings					◎	
	Network time protocol settings					◎	
	Power off					◎	
	OTA upgrade					◎	
	Settings					◎	
	Expand status bar					◎	
	Clipboard					○	
	Share via apps					◎	
	Smart Select					○	
	Reboot banner					◎	
	Power saving mode control					◎	

	Firmware download mode control					◎	
	Samsung keyboard settings control					◎	
Connectivity	Use Printer	○	◎		◎	○	◎
	Always On VPN	○	◎	○	◎		
	Auto-Completion in Browser	○	◎			○	◎
	Send Files through Bluetooth	◎	◎			◎	◎
	5G network slicing	○	◎		◎	○	◎
	Reset Mobile Data Usage	○				○	
	Configure Mobile Network Settings	◎		◎		◎	
	Wi-Fi setting	◎		◎		◎	
	Use Wi-Fi (including Wi-Fi direct)	◎				◎	
	Wi-Fi SSID allowlist setting	○				◎	
	Wi-Fi SSID blocklist setting	○				◎	
	Share Internet Connection Using Tethering	◎		◎		◎	
	Use Bluetooth	◎		◎		◎	◎
	Control Bluetooth settings	◎		◎		◎	
	Transfer files through USB	◎				◎	
	Use external SD card	◎				◎	
	USB debugging		◎			◎	◎
	NFC control					○	
	USB host storage(OTG) (including Set USB exception allowed list)					◎	
	Wi-Fi hotspot					◎	
	Wi-Fi auto connection					◎	
	Wi-Fi minimum security level setting					◎	
	USB tethering					◎	
	Bluetooth tethering					◎	
	Bluetooth UUID allowlist setting					◎	
	Bluetooth UUID blocklist setting					◎	
	Allow USB devices for default access by app					○	◎
Security	Check Devices through Play Integrity	○	◎	○	○	○	◎
	Multi factor authentication		◎			○	
	Secure startup					○	
	Google Android security update policy					○	
Lock Screen	Screen lock policies	◎	◎	◎	◎	◎	◎
	Block certain actions if screen is locked	◎	◎	◎	◎	◎	◎
	Set maximum screen timeout allowed	○	◎	○	◎	○	
	Screen lock time changes by device user	○				○	
Kiosk	Single app mode	○		○		○	
	Multi app mode	○		○		○	
	Web mode	○				○	
	Delete kiosk app when policy is removed	○				○	
	Turn Screen on when Plugged in	○		○		○	
App Restriction	App Installation from other sources	○	◎	◎	◎	○	◎
	Skip app tutorial	○	◎		◎	○	◎
	Control apps from settings	○	◎			○	◎
	App installation	○	◎		◎	○	◎
	App uninstallation	○	◎		◎	○	◎
	App verification using Google Play Protect	○	◎		◎	○	◎
	Runtime permissions for all apps	○	◎	◎	◎	○	◎
	Block certain apps from running	○	◎	○	◎	◎	◎
	Hide apps	◎	◎			◎	◎

	Block certain apps from being uninstalled	○	◎			○	◎
	Activate certain pre-installed system apps	○	◎		◎	○	◎
	Delegated scopes for apps	○	◎	◎	◎	○	◎
	Block certain apps from using mobile data	○	◎			○	◎
	Allow or block certain apps from downloading	◎				○	
	Apps allowing external SD card		◎				◎
	Allow work and Personal apps connection		◎		◎		
	Google Play protect verify apps				◎		
	Play store mode			◎	◎		
	Battery optimization exceptions					○	
	Block components from running in certain apps					○	○
	Add work profile apps to home screen widgets		◎				
Location	Location Settings	◎	◎			◎	◎
	Location Mode				◎		
Phone	Turn on airplane mode	◎		◎		◎	
	Emergency Alerts	◎		◎		◎	
	Adjust volume	○				○	
	Use Microphone	◎		◎		◎	
	Make Voice Calls on Non-Samsung Devices	◎				◎	
	Send Text Messages on Non-Samsung Devices	◎				◎	
	Data connection during roaming	◎		◎		◎	
	Contact management	◎	◎			◎	
	Prohibit voice call(Incoming/Outgoing)			◎		◎	
	Disallow SMS/MMS(Incoming/Outgoing)			◎		◎	
	WAP push during roaming					◎	
	Data sync during roaming					◎	
	Voice calls during roaming					◎	
	Use SIM card locking					○	
Container	Copy and paste clipboard per profile		◎		◎		
	Phone Book Access Profile(PBAP) via Bluetooth		◎		◎		
	Set a message for profile wipe		◎		◎		
	Set a maximum period for profile turn off		◎		◎		
Factory Reset Protection	Factory reset protection	◎	◎	◎	◎	○	
Knox Browser	Homepage URL	◎	◎			◎	◎
	App auto updates	◎	◎			◎	◎
	Hide URL address bar	◎	◎			◎	◎
	Add URLs to allowlist or blocklist	◎	◎			◎	◎
	URLs	◎	◎			◎	◎
	Web intents	◎	◎			◎	◎
	Store cookies	◎	◎			◎	◎
	Download files	◎	◎			◎	◎
	Upload files	◎	◎			◎	◎
	Copy text	◎	◎			◎	◎
	Screen capture	◎	◎			◎	◎
	Add Bookmarks	◎	◎			◎	◎
	Text scaling	◎	◎			◎	◎
	Force page zoom	◎	◎			◎	◎
Staging	Staging device settings	○				○	
Browser	Cookies					○	
	JavaScript					○	
	Auto fill					○	

	Pop-up block					○	
	Browser proxy URL					○	
Custom Animation	Boot animation					◎	
	Shutdown animation					◎	
Firewall	Permitted policy (IP)					◎	
	Prohibited policy (IP)					◎	
	Permitted policy (Domain)					◎	
	Prohibited policy (Domain)					◎	
	DNS setting					◎	
DeX	DeX mode					◎	
	Ethernet only					○	
	Application execution blocklist (Android)					○	
Knox Service Plugin	Provide the same feature set by Knox Service Plugin dynamic UI and Knox Service Plugin premium features are available with Knox Suite license of Knox Platform for Enterprise license Please refer to samsungknox.com for the KSP feature list (https://docs.samsungknox.com/dev/knox-service-plugin/index.htm)						
Settings	Wi-Fi	○		○		○	
	Shortcut	○				○	
	APN	○				○	
	Certificate	○				○	
	Google account	○				○	

2. iOS & iPadOS

Category	Feature	Supported
System	Camera	○
	Screen capture	○
	Siri	○
	Force on device only dictation (Siri)	○
	Force on device only translation (Siri)	○
	Submission of diagnosis and usage details	○
	Passbook on lock scree	○
	Control center on lock screen	○
	Display notification on lock screen	○
	Display today view on lock screen	○
	Manual installation for profile	○(Supervised)
	Control editing account information	○(Supervised)
	Automatic updates of certificate trust settings	○
	Encryption for iTunes backup	○
	iTunes pairing	○(Supervised)
	Apple Watch paring	○(Supervised)
	Wrist detection on an Apple Watch	○
	Limit Ad tracking	○
	Apple personalized advertising	○
	Factory reset	○(Supervised)
	Result of web search with spotlight	○
	Block configuration	○(Supervised)
	Change device name	○(Supervised)
	Device name modification	○(Supervised)
	Bluetooth modification	○(Supervised)
	Automatic data and time	○(Supervised)
	VPN creation	○(Supervised)
	Wallpaper modification	○(Supervised)

	Custom wallpaper	○(Supervised)
	Notifications modification	○(Supervised)
	New device proximity setup	○(Supervised)
	Unpaired external boot to recovery	○(Supervised)
	Keyboard shortcuts	○(Supervised)
	Predictive keyboard	○(Supervised)
	Auto correction for keyboard	○(Supervised)
	Spell-check for keyboard	○(Supervised)
	Definition lookup for keyboard	○(Supervised)
	QuickPath keyboard	○(Supervised)
	Dictation	○(Supervised)
	Rapid security response installation	○(Supervised)
	Rapid security response removal	○(Supervised)
	iPhone widgets on Mac devices	○(Supervised)
	iPhone mirroring	○(Supervised)
	Personalized Handwriting	○(Supervised)
	Genmoji	○(Supervised)
	Image Playground	○(Supervised)
	Image Wand	○(Supervised)
	Writing Tools	○(Supervised)
	Apple intelligence report	○(Supervised)
	Mail smart reply	○(Supervised)
	Mail summary	○(Supervised)
Connectivity	USB drive access	○(Supervised)
	Network device access	○(Supervised)
	USB restricted mode	○(Supervised)
	NFC	○(Supervised)
	Wi-Fi On	○(Supervised)
	Connect Wi-Fi to allowed networks only	○(Supervised)
	Personal hotspot modification	○(Supervised)
Security	Passcode policies	○
	Passcode modification	○(Supervised)
	Screen unlock with biometric ID (or Touch ID for Window)	○
	Password proximity requests	○(Supervised)
	Password autofill	○(Supervised)
	Authentication before password autofill	○(Supervised)
	Password sharing	○(Supervised)
	Auto unlock	○
App Restriction	App installation	○(Supervised)
	App uninstallation	○(Supervised)
	Automatic app download	○(Supervised)
	iTunes store	○(Supervised)
	Game center	○(Supervised)
	iBook store	○(Supervised)
	inappropriate contents download on iBook store	○
	iMessage	○(Supervised)
	YouTube	○
	Apple news	○(Supervised)
	Apple music radio	○(Supervised)
	Apple music	○(Supervised)
	Apple podcasts	○(Supervised)

	Find friends	○(Supervised)
	Find friends modification	○(Supervised)
	Find my device	○(Supervised)
	In-app purchase	○
	App block/allowlist settings	○(Supervised)
	Autonomous single app mode	○(Supervised)
	Trust enterprise app	○
	App Clips	○(Supervised)
	System app removal	○(Supervised)
	Managed apps to write contacts to unmanaged contacts accounts	○
	Unmanaged apps to read contacts from managed contacts accounts	○
	Marketplace app installation	○(Supervised)
	Web distribution app installation	○(Supervised)
	Lock apps	○(Supervised)
	Hide apps	○(Supervised)
Phone	Modification of cellular data settings for each application	○(Supervised)
	FaceTime	○(Supervised)
	Voice dialing	○
	Background fetch for roaming	○
	eSIM modification	○(Supervised)
	Cellular plan modification	○(Supervised)
	Live voicemail	○(Supervised)
	Preservation of eSIM on erase	○(Supervised)
	eSIM transfer between devices	○(Supervised)
	Call recording	○(Supervised)
	Default calling app modification	○(Supervised)
	Default messaging app modification	○(Supervised)
Share	Allow open from unmanaged to managed apps	○
	Allow open from managed to unmanaged apps	○
	Managed pasteboard	○
	AirDrop	○(Supervised)
	Consider AirDrop not managed	○(Supervised)
	AirPrint	○(Supervised)
Browser	Safari	○(Supervised)
	Cookies	○
	JavaScript	○
	Auto fill	○(Supervised)
	Block pop-ups	○
	Untrusted TLS certificate	○
	Web forgery warning	○
	Default browser modification	○(Supervised)
iCloud	Backup	○
	Document synchronization	○(Supervised)
	Enterprise book backup	○
	Enterprise books, notes and highlights sync	○
	iCloud photo library	○
	Photo stream	○
	Photo sharing	○
	Keychain synchronization	○
	Managed app synchronization	○
	Handoff	○

Media	Rating for each country	○
Settings	Software Update	○
	Software Update Enforcement	○(Supervised)
	Wi-Fi	○
	Exchange	○
	VPN(device wide / per App)	○
	Certificate	○
	SSO	○
	Cellular	○
	AirPrint	○
	Font	○
	Web Clip	○
	Home Screen Layout	○
	App Lock	○(Supervised)
	Global HTTP proxy	○(Supervised)
	AirPlay (iOS7 or above)	○
	Web content filter (iOS 7 or above)	○(Supervised)
	Managed domains (iOS 8 or above)	○
	Network usage rules (iOS 9 or above)	○

3. MacOS

Category	Feature	Supported
System	Camera	○
	Screen capture	○
	Manual installation for profile	○
	Factory reset	○
	Delay Software update	○
	App adoption by user	○
	USB restricted mode	○
Security	Password policies	○
	Passcode modification	○
	Screen unlock with Touch ID	○
	Touch ID timeout	○
iCloud	Private relay	○
	Document synchronization	○
Settings	Wi-Fi	○
	Certificate	○
	Global HTTP proxy	○

4. Windows

Category	Feature	Supported
System	Factory reset	○
	Camera	○
	Screen capture	○
	VPN	○
	VPN over cellular	○
	VPN roaming over cellular	○
	Sign in options	○
	Date and time	○

	Language	○
	Power and Sleep	○
	Region	○
	Workplace	○
	Account	○
	Windows sync	○
	Windows tips	○
Connectivity	Wi-Fi	○
	Bluetooth	○
	Bluetooth advertising	○
	NFC	○ (mobile only)
	USB	○ (mobile only)
	Removable Storage	○
	Cortana	○
	IME logging	○
	IME network access	○
Security	Password policies	○
App Restriction	Windows app store access control	○ (mobile only)
	App installation block/allowlist setting	○
	Developer unlock	○
	DVR & Game Broadcasting	○
	Restrict App Data to System Volume	○
	All trusted app(Non-Microsoft store apps)	○
	App Store Auto Updates	○
	Share App Data between Users	○
Location	Location Settings	○
Phone	Data connection during roaming	○
Administrative Templates	Computer Configuration	○
	User Configuration	○
ETC	Delete PPKG	○
	MDM client unenrollment	○
Kiosk	Single app mode	○
	Multi app mode	○
Settings	Wi-Fi	○
	Exchange	○
	VPN(device wide / per App)	○
	Certificate	○
	App Locker	○
	Proxy	○
	Windows Hello	○
	Update	○
	Custom	○

5. Wear OS

Category	Feature	Supported
System	Screen capture	○
	OTA upgrade	○
	Factory reset	○
	Developer mode	○
	Key remapping settings	○

	Power saving mode	○
	Sound mode settings	○
	Sound mode	○
	Microphone	○
	Language setting	○
	Brightness setting	○
	Brightness level	○
	Adaptive brightness	○
	Always on display	○
	Raise wrist to wake	○
	Touch screen to wake	○
	Automatic date and time	○
	Sleep mode	○
	Show emergency call button	○
	Auto fall detection	○
	Show charging info	○
	Touch sensitivity control	○
	Wrist orientation	○
	Button position	○
Connectivity	Mobile networks setting	○
	Wi-Fi	○
	NFC	○
	Bluetooth	○
Lock screen	Screen lock policy	○
Kiosk	Multi app mode	o
App restrictions	App permission	○
	App execution blocklist	○
	Hide apps	○
	App uninstallation prevention list setting	○
	App delegation scope management	○
	Watch face customization	○
	Battery optimization exceptions	○
Location	Location Mode	○
Phone	Airplane mode	○
	Data roaming	○
	Auto call answer	○
	Contact management	○
Settings	Wi-Fi	○
	APN / Cellular	○

6. ChromeOS

Category	Feature	Supported
Users & browsers - General	Maximum user session length	○
	Custom avatar	○
	Custom wallpaper	○
Users & browsers - Sign-in settings	Display password button	○
browsers - Enrollment c	Device enrollment	○
	Asset identifier during enrollment	○
	Enrollment permissions	○

Users & browsers - Apps and extensions	Task manager	○
rs & browsers - Site isola	Site isolation	○
Users & browsers - Security	Password manager	○
	Lock screen	○
	Quick unlock	○
	PIN auto-submit	○
	Lock screen media playback	○
	Idle settings	○
	Incognito mode	○
	Browser history	○
	Clear browser history	○
	Online revocation checks	○
	Geolocation	○
	Single sign-on	○
	SAML single sign-on login frequency	○
	Allowed certificate transparency URLs	○
	Certificate transparency CA allowlist	○
	Certificate transparency legacy CA allowlist	○
	User management of installed CA certificates	○
	User management of installed client certificates	○
	CPU task scheduler	○
	Enable leak detection for entered credentials	○
	Ambient authentication	○
	Unsupported system warning	○
	Advanced protection program	○
	Override insecure origin restrictions	○
	Popup interactions	○
	Security token removal	○
Users & browsers - Remote access	Remote access clients	○
	Remote access hosts	○
	Firewall traversal	○
Users & browsers - Session settings	Show logout button in tray	○
Users & browsers - Kerberos	Kerberos tickets	○
	Remember Kerberos passwords	○
	Kerberos accounts	○
Users & browsers - Network	Proxy mode	○
	Ignore proxy on captive portals	○
	Supported authentication schemes	○
	Allow basic authentication for HTTP	○
	NTLMv2 authentication	○
	Minimum SSL version enabled	○
	SSL error override	○
	SSL error override allowed domains	○
	WebRTC UDP ports	○
	WebRTC ICE candidate URLs for local Ips	○
	QUIC protocol	○
	DNS-over-HTTPS	○
	Built-in DNS client	○
	Integrated authentication servers	○
	Kerberos delegation servers	○

	Kerberos ticket delegation	○
	Kerberos service principal name	○
	Kerberos SPN port	○
	Cross-origin authentication	○
	SharedArrayBuffer	○
	User agent client hints	○
	Signed HTTP exchange(SXG) support	○
	Globally scoped HTTP authentication cache	○
	Require online OCSP/CRL checks for local trust anchors	○
	HSTS policy bypass list	○
	CNS interception checks enabled	○
	Intranet redirection behavior	○
	Legacy TLS/DTLS downgrade in WebRTC	○
	WPAD optimization	○
	Login credentials for network authentication	○
	Allowed network ports	○
	CECPQ2 post=quantum key-agreement for TLS	○
Users & browsers - Android applications	Control Android backup and restore service	○
	Google location services	○
	Certificate synchronization	○
Users & browsers - Startup	Home button	○
	Homepage	○
	New tab page	○
	New tab page background	○
	Paged to load on startup	○
Users & browsers - Content	SafeSearch and restricted mode	○
	Screenshot	○
	Screen video capture	○
	Client certificates	○
	Security key attestation	○
	3D content	○
	Cookies	○
	Third-party cookie blocking	○
	Default legacy same site cookie behavior	○
	Per-site legacy same site cookie behavior	○
	Images	○
	JavaScript	○
	JavaScript intentiveWakeUp throttling	○
	Notifications	○
	Autoplay video	○
	Auto open download files	○
	Pop-ups	○
	Cross-origin JavaScript dialogs	○
	URL blocking	○
	Google Drive syncing	○
	Google Drive syncing over cellular	○
	Cast	○
	Control use of insecure content exceptions	○
	Allow insecure content on these sites	○
	Block insecure content on these sites	○
	Insecure forms	○

	Network file shared	○
	Scroll to text fragment	○
	Enable URL-keyed anonymized data collection	○
	AppCache	○
	Web Bluetooth API	○
	PDF annotations	○
	File handling API	○
Users & browsers - Printing	Enable/Disable Printing	○
	Deprecated privet printing	○
	Print preview default	○
	Printer management	○
	Default color printing mode	○
	Restrict color printing mode	○
	Default page sides	○
	Restrict page sides	○
	Background graphics printing default	○
	Background graphics printing restriction	○
	CUPS print job information	○
	Print job history retention period	○
	Print job history deletion	○
	Restrict PIN printing mode	○
	Default PIN printing mode	○
	Maximum sheets	○
	Default printing page size	○
	Print headers and footers	○
	Blocked printer types	○
Users & browsers - User experience	Managed bookmarks	○
	Bookmark bar	○
	Shelf position	○
	Shelf auto-hiding	○
	Bookmark editing	○
	Download location	○
	Download location prompt	○
	Spell check	○
	Spell check service	○
	Google translate	○
	Alternate error pages	○
	Developer tools	○
	Form auto-fill	○
	Payment methods	○
	Emoji suggestions	○
	Multiple sign-in access	○
	Sign-in to secondary accounts	○
	Unified Desktop(BETA)	○
	WebRTC event log collection	○
	Disabled system features	○
	Dinosaur game	○
	Previously installed app recommendations	○
	Suggested content	○
	URLs in the address bar	○
	Shared clipboard	○

	Full screen mode	○
	Full screen alert	○
	Show cards on the new tab page	○
	Maximize window on first run	○
	Allow user feedback	○
	Media recommendations	○
Users & browsers - Connected devices	Smart lock	○
	Instant tethering	○
	Messages	○
	Click to call	○
	Phone hub	○
Users & browsers - Accessibility	Spoken feedback	○
	Select to speak	○
	High contrast	○
	Screen magnifier	○
	Sticky keys	○
	On-screen keyboard	○
	Dictation	○
	Keyboard focus highlighting	○
	Caret highlight	○
	Auto-click enabled	○
	Large cursor	○
	Cursor highlight	○
	Primary mouse button	○
	Mono audio	○
	Accessibility shortcuts	○
	Accessibility options in the system tray menu	○
	Image descriptions	○
Users & browsers - Power and shutdown	Wake locks	○
Users & browsers - Omnibox search provider	Search suggest	○
Users & browsers - Hardware	External storage devices	○
	WebUSB API	○
	Audio input (microphone)	○
	Audio input allowed URLs	○
	Audio output	○
	Video input (camera)	○
	Video input allowed URLs	○
	Keyboard	○
	Serial port API	○
	Privacy screen	○
	File system read access	○
	File system write access	○
	Sensors	○
	Enterprise hardware platform API	○
Users & browsers - User verification	Verified mode	○
Users & browsers - User reporting	Managed browser reporting upload frequency	○
Users & browsers - Chrome safe browsing	Safe browsing	○
	Help improve safe browsing	○

	Safe browsing allowed domains	○
	Download restrictions	○
	Disable bypassing safe browsing warnings	○
	Password alert	○
	Safe Sites URL filter	○
	Suppress lookalike domain warnings on domains	○
	Sites with intrusive ads	○
	Abusive experience intervention	○
Users & browsers - Chrome updates	Component updates	○
Users & browsers - Virtual machines (VMs) and developers	Command line access	○
	Linux virtual machines(BETA)	○
	Port forwarding	○
	Android apps from untrusted sources	○
Users & browsers - Parallels Desktop	Allow/Disallow to use Parallels Desktop	○
	Parallels Desktop windows image	○
	Required disk space	○
	Diagnostic information	○
Users & browsers - Other settings	Policy fetch delay	○
	Wi-Fi network configurations sync	○
Device - Enrollment and access	Forced re-enrollment	○
	Powerwash	○
	Verified access	○
	Verified mode	○
	Disabled device return instructions	○
	Integrated FIDO second factor	○
Device - Sign-in settings	Guest mode	○
	Sign-in restriction	○
	Autocomplete domain	○
	Sign-in screen	○
	Device off hours	○
	Device wallpaper image	○
	User data	○
	Single sign-on IdP redirection	○
	Single sign-on cookie behavior	○
	Single sign-on camera permissions	○
	Single sign-on client certificates	○
	Accessibility control	○
	Sign-in language	○
	Sign-in keyboard	○
	Single sign-on verified access	○
	System info on sign-in screen	○
	Privacy screen on sign-in screen	○
	Show numeric keyboard for password	○
Device - Sign-in screen accessibility	Spoken feedback	○
	Select to speak	○
	High contrast	○
	Screen magnifier	○
	Sticky keys	○

	On-screen keyboard	○
	Dictation	○
	Keyboard focus highlighting	○
	Caret highlight	○
	Auto-click enabled	○
	Large cursor	○
	Cursor highlight	○
	Primary mouse button	○
	Mono audio	○
	Accessibility shortcuts	○
Device - Device update settings	Auto-update settings	○
	App-controlled updates	○
	Kiosk-controlled updates	○
	Release channel	○
	Variations	○
	Update downloads	○
Device - User and device reporting	Report device OS information	○
	Report device hardware information	○
	Report device telemetry	○
	Report kiosk session status	○
	Report the running kiosk app	○
	Report device print jobs	○
	Report status report upload frequency	○
	Inactive device notifications	○
	Anonymous metric reporting	○
	Device system log upload	○
Device - Display settings	Screen settings	○
Device - Power and shutdown	Power management	○
	Scheduled reboot	○
	Allow shutdown	○
Device - Virtual machines	Linux virtual machines for unaffiliated users (BETA)	○
	Android apps from untrusted sources	○
Device - Other settings	Device network hostname template	○
	Timezone	○
	Mobile data roaming	○
	USB access	○
	Bluetooth	○
	Bluetooth services allowed	○
	Throttle device bandwidth	○
	TPM firmware update	○
	Authenticated Proxy Traffic	○
	System clock format	○
	Apps and extensions cache size	○
	Hardware profiles	○
	Low disk space notification	○
	Redeem offers through Chrome OS registration	○
Device - Imprivata	Imprivata login screen integration	○
Managed guest sessions - General	Managed guest session	○
	Maximum user session length	○
	Custom terms of service	○
	Custom avatar	○

	Custom wallpaper	○
Managed guest sessions - Apps and extensions	Task manager	○
Managed guest sessions - Security	Idle settings	○
	Incognito mode	○
	Browser history	○
	Browsing data lifetime	○
	CPU task scheduler	○
	Unsupported system warning	○
	Override insecure origin restrictions	○
	Pop-ups interactions	○
	Security token removal	○
	Screen brightness	○
	Allow remote debugging	○
	Insecure media capture	○
	WebSQL in third-party context	○
Managed guest sessions - Remote	Remote access clients	○
	Remote access hosts	○
Managed guest sessions - Session settings	Show logout button in tray	○
	Display the logout confirmation dialog	○
Managed guest sessions - Kerberos	Kerberos tickets	○
Managed guest sessions - Network	Proxy mode	○
	Ignore proxy on captive portals	○
	Minimum SSL version enabled	○
	SSL error override	○
	SSL error override allowed domains	○
	QUIC protocol	○
	WebRTC IP handling	○
	DNS-over-HTTPS	○
	Built-in DNS client	○
	Integrated authentication servers	○
	SharedArrayBuffer	○
	User-Agent client hints	○
	Signed HTTP exchange(SXG) support	○
	Globally scoped HTTP authentication cache	○
	Require online OCSP/CRL checks for local trust anchors	○
	HSTS policy bypass list	○
	DNS interception checks enabled	○
	Intranet redirection behavior	○
	Legacy TLS/DTLS downgrade in WebRTC	○
	WPAD optimization	○
	Allowed network ports	○
	CECPQ2 post=quantum key-agreement for TLS	○
	DNS queries for additional DNS record types	○
	User-Agent client hints	○
Managed guest sessions - Startup	Home button	○
	Homepage	○
	New tab page	○
	Pages to load on startup	○

	Browser launch on startup	○
Managed guest sessions - Content	SafeSearch and restricted mode	○
	Screenshot	○
	Screen video capture allowed by sites	○
Managed guest sessions - Printing	Printing	○
	Deprecated privet printing	○
	Print preview default	○
	Printer management	○
	Default color printing mode	○
	Restrict color printing mode	○
	Default page sides	○
	Restrict page sides	○
	Background graphics printing default	○
	Background graphics printing restriction	○
	Print job history retention period	○
	Print job history deletion	○
	Restrict PIN printing mode	○
	Default PIN printing mode	○
	Maximum sheets	○
	Default printing page size	○
	Print headers and footers	○
	Blocked printer types	○
Managed guest sessions - User experience	Managed bookmarks	○
	Bookmark bar	○
	Shelf position	○
	Download location prompt	○
	Download bubble	○
	Spell check	○
	Spell check service	○
	Allowed ChromeOS languages	○
	Allowed input methods	○
	Google translate	○
	Developer tools	○
	Payment methods	○
	Session locale	○
	Emoji suggestions	○
	Unified Desktop(BETA)	○
	Disabled system features visibility	○
	Disabled system features	○
	Dinosaur game	○
	Previously installed app recommendations	○
	Suggested content	○
	URLs in the address bar	○
	Fullscreen mode	○
	Fullscreen after unlock	○
	Maximize window on first run	○
	Allow user feedback	○
	Persist display settings	○
	Lock icon in the omnibus for secure connections	○
	URL parameter filtering	○
	ChromeOS color mode	○

Managed guest sessions - Accessibility	Spoken feedback	○
	Select to speak	○
	High contrast	○
	Screen magnifier	○
	Sticky keys	○
	On-screen keyboard	○
	On-screen keyboard in tabled mode	○
	Dictation	○
	Keyboard focus highlighting	○
	Caret highlight	○
	Auto-click enabled	○
	Large cursor	○
	Cursor highlight	○
	Primary mouse button	○
	Mono audio	○
	Accessibility shortcuts	○
	Accessibility options in the system tray menu	○
	Image descriptions	○
Managed guest sessions - Power and shutdown	Wake locks	○
Managed guest sessions - Omnibox search provider	Search suggest	○
Managed guest sessions - Hardware	External storage devices	○
	WebUSB API	○
	Audio input (microphone)	○
	Audio input allowed URLs	○
	Audio output	○
	Video input(camera)	○
	Video input allowed URLs	○
	Keyboard	○
	Serial Port API	○
	Privacy screen	○
	File system read access	○
	File system write access	○
	Sensors	○
	Enterprise hardware platform API	○
Managed guest sessions - Chrome safe browsing	Download restrictions	○
	Disable bypassing safe browsing warnings	○
	SafeSites URL filter	○
	Suppress lookalike domain warnings on domains	○
	Sites with intrusive ads	○
	Abusive experience intervention	○
Managed guest sessions - Other settings	Policy fetch delay	○
	Fast pair(fast Bluetooth pairing)	○
Kiosk settings	Managed guest session	○
	Kiosk device status alerting delivery	○
	Kiosk device status alerting contact info	○
	URL blocking	○

Kiosk power settings	Action on lid close	○
	AC kiosk power settings	○
	Battery kiosk power settings	○
Kiosk accessibility	Kiosk floating accessibility menu	○
	Kiosk spoken feedback	○
	Kiosk select to speak	○
	Kiosk high contrast	○
	Kiosk sticky keys	○
	Kiosk on-screen keyboard	○
	Kiosk dictation	○
	Kiosk keyboard focus highlighting	○
	Kiosk caret highlight	○
	Kiosk auto-click enabled	○
	Kiosk large cursor	○
	Kiosk cursor highlight	○
	Kiosk primary mouse button	○
	Kiosk mono audio	○
	Kiosk accessibility shortcuts	○
	Kiosk screen magnifier	○
Apps & extensions - Additional settings	Allow/block mode (Play Store, Chrome Web Store)	○
	Android applications on Chrome devices	○
	Allowed types of apps and extensions	○
	App and extension install sources	○
	Allow insecure extension packaging	○
	External extensions	○
	Permissions and URLs	○
	Chrome Web Store app icon	○
	Chrome Web Store homepage	○
	Chrome Web Store permissions	○
	Android reporting for users and devices	○
	Full restore	○
	Android ghost windows	○
Chrome management - partner access	Allow EMM partners access to device management	○
Settings	Wi-Fi	○
	VPN(device wide / per App)	○
	Ethernet	○
	General settings (Chrome book only)	○

Original console

Device commands

1. Android Enterprise

Category	Feature	Android Enterprise					
		Fully managed	Work profile on company-owned	Work profile	Shared (Temporary)	Shared (Persistent)	Non-shared
Device	Push Profile	○	○	○	○	○	○
	Lock Device	○			○	○	○
	Unlock Device	○			○	○	○
	Lock Screen	○			○	○	○
	Lock SIM PIN	○	○				
	Unlock SIM PIN	○	○				
	Activate eSIM cellular plan	○	○	○	○	○	
	Remove eSIM cellular plan	○	○	○	○	○	
	Collect EID information			○			
	Factory Reset	○			○	○	○
	Power Off Device	○			○	○	○
	Reboot Device	○			○	○	○
	Clear Screen Lock	○					
	Reset SD Card	○					
	Reset Data Usage	○					
	Reset Number of Calls	○	○				
	Delete a CA Certificate	○					
	Delete a User Certificate	○					
	Delete a User Install Certificate	○					
	Delete a Work Profile CA Certificate		○	○			
	Delete a Work Profile User Certificate		○	○			
	Delete a Work Profile User Install Certificate		○	○			
App mgmt.	Install or Update App	○	○	○	○	○	○
	Run App	○	○	○			
	Uninstall App	○	○	○	○	○	○
	Apply Latest Internal App Information	○					
	Delete App Data	○	○	○	○	○	○
Work profile controls	Clear (Reset) Work Profile Password		○	○			
	Lock Screen		○	○			
Knox Manage	Push Notification	○	○	○			
	Unenroll Device	○	○	○	○	○	○
	Update License	○	○	○	○	○	○
	Update Knox Manage Agent	○	○	○	○	○	○
	Update User Information	○	○	○			
	Lock Screen of Knox Manage Agent	○	○	○			
	Unlock Knox Manage Agent	○	○	○			
	Exit Kiosk Mode	○					
	Exit Shared Device Mode				○	○	
	Exit Non-Shared Device Mode						○

	Collect Audit Log	○	○	○	○	○	○
	Collect Device Diagnostics Log	○	○	○	○	○	○
	Collect Bug Report	○			○	○	○
	Reset Push Token	○		○	○	○	○
	Delete User Data					○	
	Register Managed Google Play Account	○	○	○			
	Upgrade to managed Google account	○	○	○			
	Play Alarm Sound	○	○	○			
	Reapply KSP Wi-Fi Configurations	○	○				
Device info.	Collect Current Location	○	○	○			
	Sync Device Information	○	○	○	○	○	
	Sync Installed App List	○	○	○	○	○	
	Authenticate SIM Card	○					
	Attestation	○					
	Play Integrity (SafetyNet Attestation)	○	○	○			

2. Android Enterprise - Android Management API

Category	Feature	Android Enterprise - Android Management API	
		Work profile on company-owned	Work profile
Device	Push Profile	○	○
	Clear Screen Lock	○	○
	Unenroll Device	○	○
	Enable Lost Mode	○	
	Disable Lost Mode	○	
Application	Delete App Data	○	○
Work profile controls	Lock Screen	○	○

3. Android Legacy, Knox workspace, Fully managed with work profile

Category	Feature	Android Legacy				
		Legacy	Legacy with Knox workspace		Fully managed with Work profile	
			Device	Workspace	Device	Workspace
Device	Push Profile	○	○	○	○	○
	Lock Device	○	○		○	
	Unlock Device	○	○		○	
	Lock Screen	○	○		○	
	Lock SIM PIN	○	○		○	
	Unlock SIM PIN	○	○		○	
	Factory Reset	○	○		○	
	Power Off Device	○	○		○	
	Reboot Device	○	○		○	
	Clear Screen Lock	○	○		○	
	Reset SD Card	○	○		○	
	Reset Data Usage	○	○		○	
	Reset Number of Calls	○	○		○	
	Delete a CA Certificate				○	
	Delete a User Certificate				○	

	Delete a User Install Certificate				○	
	Delete a Work Profile CA Certificate					○
	Delete a Work Profile User Certificate					○
	Delete a Work Profile User Install Certificate					○
	Remove Unauthorized Container	○	○			
App mgmt.	Install or Update App	○	○	○	○	○
	Run App	○	○	○	○	○
	Stop App	○	○	○		
	Uninstall App	○	○	○	○	○
	Apply Latest Internal App Information	○	○	○	○	
	Delete App Data	○	○	○	○	○
	Enable App Running	○	○			
	Disable App Running	○	○			
Container	Clear (Reset) Work Profile Password			○		○
	Lock Screen					○
	Lock Knox Workspace			○		
	Unlock Knox Workspace			○		
	Uninstall Knox Workspace			○		
Knox Manage	Push Notification	○	○	○	○	○
	Unenroll Device	○	○		○	
	Update License	○	○		○	○
	Update Knox Manage Agent	○	○		○	
	Update User Information	○	○	○	○	○
	Lock Screen of Knox Manage Agent	○	○	○	○	○
	Unlock Knox Manage Agent	○	○	○	○	○
	Exit Kiosk Mode	○	○			
	Change License				○	○
	Collect Audit Log	○	○	○	○	○
	Collect Device Log	○	○	○	○	○
	Collect Device Diagnostics Log	○	○	○	○	○
	Collect Bug Report				○	
	Reset Push Token	○	○		○	
	Register Managed Google Play Account					○
	Switch to Fully Managed (Remove Work Profile)				○	
Device info.	Collect H/W Status					○
	Collect Current Location	○	○			
	Sync Device Information	○	○			○
	Sync Installed App List	○	○			○
	Authenticate SIM Card	○	○			
	Authenticate SD Card	○	○			
	Attestation	○	○			

5. iOS & iPadOS

Category	**Feature**	**iOS & iPadOS**			
		Device enrollment	**Shared iPad (Staging)**	**Shared iPad (Secondary)**	**User enrollment**
Device	Push Profile	○	○	○	O

	Lock Profile	○	○	○	O
	Unlock Device	○	○		O
	Factory reset	○	○		
	Power Off Device(Supervised)	○	○		
	Reboot Device (Supervised)	○	○		
	Clear Screen Lock	○			
	Initialize Blocked Information(Supervised)	○			
	OS Update (Supervised)	○	○		
	Enable Lost Mode (Supervised)	○	○		
	Disable Lost Mode (Supervised)	○	○		
	Play Lost Mode Sound	○	○		
	Save User Information		○		
	Check User Out		○		
	Update eSIM Cellular Plan	○	○		
	Enable Activation Lock	○			
	Delete user account		○		
Application	Install or Update App	○	○		
	Uninstall App	○	○		
	Apply latest internal app info	○		○	
Knox Manage	Push Notification	○		○	
	Unenroll Device	○	○		○
	Update Knox Manage Agent	○	○		
	Update User Information	○		○	
	Lock Screen of Knox Manage Agent	○		○	
	Unlock Knox Manage Agent	○		○	
	Collect Audit Log	○		○	
	Collect Device Log	○		○	
	Collect Diagnosis information	○		○	
	Sync App Auto-removal Property (When service is deactivated)	○			
	Collect Current Location	○		○	
Device info Sync	Sync Device Information	○	○		○
	Sync Installed App List	○	○		
	Check Connection Status	○	○	○	○
	Collect Profile ID	○	○	○	○

6. macOS

Category	Feature	macOS
Device	Push profile	○
	Lock device	○
	Factory reset	○
	Power off device	○
	Reboot device	○
App mgmt.	Install or Update App	○
	Uninstall	○
Knox Manage	Unenroll service	○
Device info Sync	Sync device information	○
	Sync Installed app list	○

7. Windows

Category	Feature	Windows
Device	Push profile	○
	Lock/Unlock device	○ (mobile only)
	Lock screen	○
	Factory reset	○
	Enterprise wipe	○
	Reboot device	○
App mgmt.	Install or Update App	○
	Uninstall	○
	Apply latest internal app info	○ (mobile only)
Knox Manage	Unenroll service	○
	Push notification	○
	Unlock/Unlock screen of Knox Manage Agent	○
	Delete account	○
	Update user information	○
Device info Sync	Sync device information	○
	Sync Installed app list	○
	Collect current location	○
Custom Control	Select	○

8. Wear OS

Category	Feature	Wear OS
Device	Push profile	○
	Lock/Unlock device	○
	Clear screen lock	○
	Factory reset	○
	Reboot device	○
App mgmt.	Run App	○
	Delete app data	○
Knox Manage	Unenroll service	○
	Exit kiosk	○
	Collect audit logs	○
	Collect logs	○
	Update Knox Manage	○
	Collect Bug Report	○
	Reset push token	○
	Push notification	○
Device info Sync	Sync device information	○
	Sync Installed app list	○

9. ChromeOS

Category	Feature	Chrome
Device	Lock device	○
	Unlock device	○
	Unenroll device with factory reset	○
	Unenroll device but keeping data	○
	Factory reset	○
	Clear user profile	○
	Export logs	○

	Capture logs	○
	Reboot	○
Kiosk	Take a screenshot	○
	Set volume	○