Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
App Store, Doc Viewing, Gaming										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block viewing corporate documents in unmanaged apps	Allow Open From Managed To Unmanaged									
Allow unmanaged apps to read from managed contacts accounts	Allow Unmanaged To Read Managed Contacts									
Treat AirDrop as an unmanaged destination	Force AirDrop Unmanaged									
Block viewing non-corporate documents in corporate apps	Allow Open From Unmanaged To Managed									
Allow copy/paste to be affected by managed open-in	Require Managed Pasteboard									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Require iTunes Store password for all purchases	Force iTunes Store Password Entry (Deprecated)									
Block in-app purchases	Allow In App Purchases									
Block download of explicit sexual content in Apple Books	Allow Bookstore Erotica									
Allow managed apps to write contacts to unmanaged contacts accounts	Allow Managed To Write Unmanaged Contacts									
Ratings region	Rating Region									
No region configured										
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block App store	Allow UI App Installation									
Block installing apps using App Store	Allow App Installation									
Block automatic app downloads	Allow Automatic App Downloads									
Block playback of explicit music, podcast, and iTunes U	Allow Explicit Content									
Block adding Game Center friends	Allow Adding Game Center Friends									
Block Game Center	Allow Game Center									
Block multiplayer gaming in the Game Center	Allow Multiplayer Gaming									
Block access to network drive in Files app	Allow Files Network Drive Access									
Autonomous Single App Mode										
Apps you add to this list and assign to a device can lock the device to run only that app once launched, or lock the device while a certain action is running (for example taking a test). Once the action is complete, or you remove the restriction, the device returns to its normal state.	Autonomous Single App Mode Permitted App IDs									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Import										
Export										
App name										
App Bundle ID										
Built-in apps										
Built-in apps										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block Siri	Allow Assistant									
Block Siri while device is locked	Allow Assistant While Locked									
Require Safari fraud warnings	Safari Force Fraud Warning									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block internet search results from Spotlight	Allow Spotlight Internet Results									
Safari cookies	Safari Accept Cookies									
Allow all cookies, and allow cross site tracking										
Block Safari JavaScript	Safari Allow Java Script									
Block Safari pop-ups	Safari Allow Popups									
Block Siri for dictation	Force On Device Only Dictation									
Block Siri for translation	Force On Device Only Translation									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block camera	Allow Camera									
Block FaceTime	Allow Video Conferencing									

Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
Require Siri profanity filter	Force Assistant Profanity Filter									
Block user-generated content in Siri	Allow Assistant User Generated Content									
Block Apple News	Allow News									
Block Apple Books	Allow Bookstore									
Block iMessage	Allow Chat									
Block Podcasts	Allow Podcasts									
Music service	Allow Music Service									
Block iTunes Radio	Allow Radio Service									
Block iTunes store	Allow iTunes									
Block Find My iPhone	Allow Find My Device									
Block Find My Friends	Allow Find My Friends									
Block user modification to the Find My Friends settings	Allow Find My Friends Modification									
Block removal of system apps from device	Allow System App Removal									
Block Safari	Allow Safari									
Block Safari Autofill	Safari Allow Autofill									
Cloud and Storage										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Force encrypted backup	Force Encrypted Backup									
Block managed apps from storing data in iCloud	Allow Managed Apps Cloud Sync									
Block backup of enterprise books	Allow Enterprise Book Backup									
Block notes and highlights sync for enterprise books	Allow Enterprise Book Metadata Sync									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block iCloud Photos sync										
Block iCloud Photo Library	Allow Cloud Photo Library									
Block My Photo Stream	Allow Photo Stream (Deprecated)/Allow Shared Stream									
Block Handoff	Allow Activity Continuation									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block iCloud backup	Allow Cloud Backup									
Block iCloud document and data sync	Allow Cloud Document Sync									
Block iCloud Keychain sync	Allow Cloud Keychain Sync									
Block iCloud Private Relay	Allow Cloud Private Relay									
Connected devices										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Force Apple Watch wrist detection	Force Watch Wrist Detection									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Require AirPlay outgoing requests pairing password	Force AirPlay Outgoing Requests Pairing Password									
Block Apple Watch auto unlock	Allow Auto Unlock									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block AirDrop	Allow AirDrop									
Block pairing with Apple Watch	Allow Paired Watch									
Block modifying Bluetooth settings	Allow Bluetooth Modification									
Block pairing with non-Configurator hosts	Allow Host Pairing									
Block AirPrint	Allow AirPrint									
Block storage of AirPrint credentials in Keychain	Allow AirPrint Credentials Storage									
Block										
Require AirPrint to destinations with trusted certificates	Force AirPrint Trusted TLS Requirement									
Block iBeacon discovery of AirPrint printers	Allow AirPrint iBeacon Discovery									
Block setting up new nearby devices	Allow Proximity Setup To New Device									
Block access to USB drive in Files app	Allow Files USB Drive Access									
Disable near-field communication (NFC)	Allow NFC									
Allow users to boot devices into recovery mode with unpaired devices	Allow Unpaired External Boot To Recovery									
Domains										

Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Unmarked email domains		Email Domains								
Managed Safari web domains		Web Domains								
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Safari password domains		Safari Password Auto Fill Domains								
General										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block sending diagnostic and usage data to Apple	Allow Diagnostic Submission									
Block screenshots and screen recording	Allow Screen Shot									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block untrusted TLS certificates	Allow Untrusted TLS Prompt									
Block over-the-air PKI updates	Allow OTAPKI Updates									
Force limited ad tracking	Force Limit Ad Tracking									
Block trusting new enterprise app authors	Allow Enterprise App Trust									
Limit Apple personalized advertising	Allow Apple Personalized Advertising									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block modification of diagnostics settings	Allow Diagnostic Submission Modification									
Block remote AirPlay, view screen by Classroom app, and screen sharing	Allow Remote Screen Observation									
Allow Classroom app to perform AirPlay and view screen without prompting	Force Classroom Unprompted Screen Observation									
Block modification of account settings	Allow Account Modification									
Block Screen Time	Allow Enabling Restrictions									
Block users from erasing all content and settings on device	Allow Erase Content And Settings									
Block modification of device name	Allow Device Name Modification									
Block modification of notifications settings	Allow Notifications Modification									
Block modification of Wallpaper	Allow Wallpaper Modification									
Block configuration profile changes	Allow UI Configuration Profile Installation									
Allow activation lock			Activation Lock Allowed While Supervised							
Block removing apps	Allow App Removal									
Block app clips	Allow App Clips									
Allow USB accessories while device is locked	Allow USB Restricted Mode									
Force automatic date and time	Force Automatic Date And Time									
Require teacher permission to leave Classroom app unmanaged classes	Force Classroom Request Permission To Leave Classes									
Allow Classroom to lock to an app and lock the device without prompting	Force Classroom Unprompted App And Device Lock									
Allow students to automatically join Classroom classes without prompting	Force Classroom Automatically Join Classes									
Block VPN creation	Allow VPN Creation									
Block modification of eSIM settings	Allow ESIM Modification									
Defer software updates	Enforced Software Update Delay									
Delay default visibility of software updates	Force Delayed Software Updates									
Keyboard and dictionary										
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block word definition lookup	Allow Definition Lookup									
Block predictive keyboards	Allow Predictive Keyboard									
Block auto-correction	Allow Auto Correction									
Block spell check	Allow Spell Check									
Block keyboard shortcuts	Allow Keyboard Shortcuts									
Block dictation	Allow Dictation									
Block QuickPath	Allow Continuous Path Keyboard									
Kiosk										
Kiosk mode locks various settings into a device, or specifies a single app that can be run on a device. This can be useful in environments like a retail store where you want a device to run only a single demo app.										

Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
App to run in kiosk mode										
Require AssistiveTouch										
Require invert colors										
Require mono audio										
Require Voice Control				Voice Control						
Require VoiceOver				Voice Over						
Require zoom				Zoom						
Block auto lock				Disable Auto Lock						
Block ringer switch				Disable Ringer Switch						
Block screen rotation				Disable Device Rotation						
Block screen sleep button				Disable Sleep Wake Button						
Block touch				Disable Touch						
Block volume buttons				Disable Volume Buttons						
Allow AssistiveTouch control				Enable Assistive Touch						
Allow invert colors control				Enable Invert Colors						
Speak on selected text				Enable Speak Selection						
Allow Voice Control				Enable Voice control						
Allow VoiceOver control				Enable Voice Over						
Allow zoom control				Enable Zoom						
Locked Screen Experience										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block Control Center access in lock screen	Allow Lock Screen Control Center									
Block Notification Center access in lock screen	Allow Lock Screen Notifications View									
Block Today view in lock screen	Allow Lock Screen Today View									
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block Wallet notifications in lock screen	Allow Passbook While Locked									
Password										
All enrollment types										
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Require password					Force PIN	Require Passcode on Device				
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block simple passwords					Allow Simple Passcode	Require Complex Passcode				
Required password type					Require Alphanumeric Passcode	Require Alphanumeric Passcode				
Alphanumeric										
Number of non-alphanumeric characters in password					Min Complex Characters	Minimum Complex Characters				
1										
Minimum password length					Min Length	Minimum Passcode Length				
Number of sign-in failures before wiping device					Max Failed Attempts	Maximum Number of Failed Attempts				
Maximum minutes after screen lock before password is required					Max Grace Period	Maximum Grace Period				
5 minutes										
Maximum minutes of inactivity until screen locks					Max Inactivity	Automatic Device Lock				
5 minutes										
Password expiration (days)					Max PIN Age In Days	Maximum Passcode Age In Days				
Prevent reuse of previous passwords					PIN History	Passcode Reuse Limit				
Block Touch ID and Face ID unlock	Allow Fingerprint For Unlock									
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block passcode modification	Allow Passcode Modification									
Block modification of Touch ID fingerprints and Face ID faces	Allow Fingerprint Modification									
Block password AutoFill	Allow Password Auto Fill									
Block password proximity requests	Allow Password Proximity Requests									

Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
Block password sharing	Allow Password Sharing									
Require Touch ID or Face ID authentication for AutoFill of password or credit card information	Force Authentication Before Auto Fill									
Restricted Apps										
Use these settings to stay informed about which users install apps that are not approved for use in your company. Select the type of restricted app list:										
Prohibited apps - A list of apps that you want to be informed about when users install them.										
Approved apps - A list of apps that are approved for use in your company. When users install an app that is not in this list, you will be informed.										
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Type of restricted apps list										
Apps list										
Import										
Export										
App store URL										
App bundle ID	Allow/Blocked Listed App Bundle IDs									
App name										
Publisher										
Shared iPad										
Shared iPad										
Configure settings for Apple Shared iPad set up with Apple Business Manager or Apple School Manager. These settings require devices running iOS 13.4 or later.										
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block Shared iPad temporary sessions	Allow Shared Device Temporary Session									
Show or Hide Apps	Allow Apps To Be Hidden									
Use the show apps list to specify the iOS apps that user can view or launch. Use the hidden apps list to specify the iOS apps that user cannot view or launch.										
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Type of apps list										
Apps list										
Import										
Export										
App store URL										
App bundle ID	Blocked App Bundle IDs									
App name										
Publisher										
Wireless										
Wireless										
Device enrollment and automated device enrollment										
These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.										
Block data roaming							Data Roaming Enabled			
Block global background fetch while roaming	Allow Global Background Fetch When Roaming									
Block voice dialing while device is locked	Allow Voice Dialing (Deprecated)									
Block voice roaming								Voice Roaming Enabled		
Block personal hotspot									Personal Hotspot Enabled	
Cellular usage rules (managed apps only)										
Block use of cellular data										Allow Cellular Data
Block use of cellular data when roaming										Allow Roaming Cellular Data
Automated device enrollment										
These settings work for supervised devices that were enrolled in Intune using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes devices supervised through Apple Configurator.										
Block changes to app cellular data usage settings	Allow App Cellular Data Modification									
Block changes to cellular plan settings	Allow Cellular Plan Modification									
Block modification of personal hotspot	Allow Personal Hotspot Modification									
Require joining Wi-Fi networks only using configuration profiles	Force WiFi To Allowed Networks Only									
Require Wi-Fi always on	Force WiFi Power On									
Require devices to use Wi-Fi networks set up via configuration profiles	Force WiFi To Allowed Networks Only									
Not listed in Template but well in Settings catalog (non exhaustive)										

Retsrictions template	Settings Catalog / Restriction	Settings Catalog / networking / domains	Settings Catalog / managed settings MDM options	Settings Catalog / App Managament / App Lock	Settings Catalog / Security / Passcode	Settings Catalog / Declarative Device Management / Passcode	Settings Catalog / Managed Settings Data Roaming	Settings Catalog / Managed Settings Voice Roaming	Settings Catalog / Managed Settings Personal Hotspot	Settings Catalog / Network Usage Rules
	Allow Apps To Be Locked									
	Allow Auto Dim									
	Allow Call Recording									
	Allow Default Browser Modification									
	allow ESIM Outgoing Transfers									
	Allow External Intelligence Integrations									
	Allow External Intelligence Integrations Sign In									
	allow Genmoji									
	Allow Image Playground									
	Allow Image Wand									
	Allow iPhone Mirroring									
	Allow iPhone Widgets On Mac									
	Allow Live Voicemail									
	Allow Mail Privacy Protection									
	Allow Mail Summary									
	allow Marketplace App Installation									
	Allow Personalized Handwriting Results									
	Allow Rapid Security Response Installation									
	Allow Rapid Security Response Removal									
	Allow RCS Messaging									
	Allow Video Conferencing Remote Control (Deprecated)									
	allow Web Distribution App Installation									
	Allow Writing Tools									
	Force Preserve ESIM On Erase									
	Declarative Device Management / Math Settings									
	Declarative Device Management / Safari Extensions									
	Declarative Device Management / Software Update Settings									
	Managed Settings / Bluetooth									
	Managed Settings / Data Roaming									
	Managed Settings / Time Zone									