ZENworks Device Control Policy Settings

Device Control Policy Settings

This section provides a detailed description of the Mobile Device Control Policy settings that can be applied on Android devices.

NOTE: This document contains updates related to the 2020 Update 1 release. To view the changes made in this release, see the Doc Updates section.

Apple Devices

The settings that can be enabled or disabled for iOS and iPadOS devices are as follows. Some of these restrictions are applicable for supervised devices only, which can be identified based on the check mark under the **Supervised Only** column:

NOTE: The settings displayed in the following table are applicable for the iPadOS platform (iPad devices with iOS version 13 and newer) as well.

Tab	Settings	Description	Applicable from
Device	Allow camera	Determines whether to enable or disable the device camera. If set to **No,** the camera icon is removed from the home screen on the device.	
	Allow FaceTime	Determines whether to enable or disable FaceTime. This setting is enabled if the **Allow camera** setting is configured as **Yes** or **Inherit.**	

Tab	Settings	Description	Applicable from
	Allow global background fetch while roaming	Determines whether the latest app data should be fetched from the network for apps running in the background, while the device is roaming.	
	Allow Handoff	Determines whether a user is allowed to resume an existing task or is allowed to access content from any device, which is logged into the same iCloud account.	
	Allow Siri	Determines whether Apple's voice assistant should be enabled.	
	Allow Siri while device is locked	Determines whether the user can access Siri while the device is locked. This setting is enabled if the **Allow Siri** setting is set to **Yes** or **Inherit.** Also, this option is ignored if a passcode is not set on the device.	iOS 5.1+
	Enable Siri profanity filter	Determines whether the Profanity Filter option in Siri should be enabled. This setting is enabled if the **Allow Siri** setting is set to **Yes** or **Inherit.**	
	Show user-generated content in Siri	Determines whether Siri can obtain content from sources that allow user-generated content, such as Wikipedia. This setting is enabled if the **Allow Siri** setting is set to **Yes** or **Inherit.**	iOS 7.0+
	Allow iMessage	Determines whether the user can use the iMessage feature on devices.	iOS 6.0+
	Allow AirDrop	Determines whether the user can share documents, media, and so on, using AirDrop.	iOS 7.0+
	Allow iBooks Store	Determines whether the user can download content from iBooks Store.	iOS 6.0+

Tab	Settings	Description	Applicable from
	Allow automatic updates to certificate trust settings	Determines whether automatic updates to certificate trust settings should be enabled.	
	Allow documents from managed sources in unmanaged destinations	Determines whether a document can be opened in an unmanaged app or account if the document was created or downloaded from a managed app or account.	iOS 7.0+
	Allow managed apps to write contacts to unmanaged apps	Determines whether managed apps can write contacts to unmanaged contacts accounts. This field is enabled, if **Allow documents from managed sources in unmanaged destinations** is enabled.	iOS 12.0+
	Allow documents from unmanaged sources in managed destinations	Determines whether a document can be opened in a managed app or account if the document was created or downloaded from an unmanaged app or account.	iOS 7.0+
	Allow unmanaged apps to access contacts in managed apps	Determines whether unmanaged apps can access managed contacts accounts. This field is enabled, if **Allow documents from unmanaged sources in managed destinations** is enabled	iOS 12.0+
	Allow screenshots	Determines whether the user can capture images of the device's display screen. If disabled, this setting will prevent the classroom app from observing remote screens.	iOS 9.0+
	Allow screen observation by Classroom	Determines whether remote screen observation by the Classroom app is enabled. This setting will be enabled, only if the **Allow screenshots** setting is enabled.	iOS 9.3+

Tab	Settings	Description	Applicable from
	Allow account modification	Determines whether the user is allowed to modify account settings, such as adding or removing mail account, modifying iCloud settings and so on.	iOS 7.0+
	Allow erase All content And settings	Determines whether the user can erase all the content and settings on the device.	
	Allow device name modification	Determines whether the user can modify the name of the device.	iOS 9.0+
	Allow host pairing	Determines whether an iOS device can pair with other devices. If No is selected, then these devices can only pair with their supervision host or with hosts having a Supervising Host Certificate. If a Supervision Host Certificate is not configured, all pairing is disabled.	iOS 7.0+
	Allow restrictions modification	Determines whether the user can modify restrictions on the device.	
	Allow Wallpaper modification	Determines whether the user can modify the wallpaper settings on the device.	iOS 9.0+
	Allow notifications modification	Determines whether the user can modify the Notification settings on the device.	iOS 9.3+
	Allow sending diagnostic and usage data to Apple	Determines whether automatic submission of diagnostic and usage reports to Apple should be enabled.	iOS 6.0+
	Allow diagnostics settings modification	Determines whether the user can modify the Diagnostic settings and app analytics settings in the Diagnostic and Usage screen on the device.	iOS 9.3.2+

Tab	Settings	Description	Applicable from
	Allow users to accept untrusted TLS certificate	Determines whether the user can accept Transport Layer Security (TLS) certificates that cannot be verified.	iOS 5.0+
	Force encrypted backup	Determines whether the device backup process should be encrypted.	
	Force limited ad tracking	Determines whether advertisers' tracking of a user's activities across apps should be limited. If set to **Yes**, then ad tracking is not eliminated but reduced to some extent.	iOS 7.0+
	Request passcode for incoming AirPlay requests	Determines whether a pairing passcode restriction should be enforced for all incoming AirPlay requests coming from another device to a managed device.	Apple TV 6.1 to tvOS 10.1
	Request passcode for outgoing AirPlay requests	Determines whether a pairing passcode restriction should be enforced for all outgoing AirPlay requests sent from a managed device to another device.	iOS 7.1+
	Treat Airdrop as unmanaged destination	Determines whether Airdrop should be considered as an unmanaged drop target. If set to **Yes**, then the user will be unable to share managed data through Airdrop.	iOS 9.0+
	Allow Spotlight Internet results	Determines whether the users can use Spotlight Search to find content directly from the Internet.	iOS and macOS 10.11+
	Allow definition lookup	Determines whether the user can lookup definitions using the in-built iOS dictionary.	iOS 8.1.3+ and macOS 10.11.2+
	Allow Dictation	Determines whether or not the user can enable the dictation option present in the keyboard.	iOS 10.3+

Tab	Settings	Description	Applicable from
	Allow VPN creation	Determines whether or not the user can configure a VPN connection using their devices.	iOS 11.0+
	Allow setting up of new devices within proximity	Determines whether the device is allowed to identify other devices that are within its proximity to share password and settings.	iOS 12.0+
	Allow automatic update of date and time	Determines whether the date and time can be automatically set based on the current location and network.	iOS 12.0+
	Allow UI configuration profile installation	Determines whether the user can install configuration profile and certificates interactively.	
Apps	Allow installation of apps	Determines whether the user can install apps.	
	Allow app installation from App Store	Determines whether the user can install apps from the Apple App Store. This field is enabled if the **Allow Installation of Apps** field is enabled. If disabled, the App Store icon is removed from the Home screen.	
	Allow automatic app downloads	Determines whether the user can automatically download apps purchased on other devices. This field is enabled if the **Allow Installation of Apps** field is enabled.	iOS 9.0+
	Allow removing apps	Determines whether the user can remove apps from the device.	
	Allow in-app purchases	Determines whether the user can make in-app purchases.	
	Allow cellular data app settings modifications	Determines whether the user can modify cellular data settings for specific apps.	iOS 7.0+

Tab	Settings	Description	Applicable from
	Allow enterprise app trust	Determines whether custom apps can be provisioned using universal provisioning profiles. If No is selected, it removes the Trust Enterprise Developer button in Settings-> General-> Profiles & Device Management. This restriction applies to free developer accounts but it does not apply to enterprise app developers who are trusted because their apps were pushed via MDM, nor does it revoke previously granted trusts.	iOS 9.0+
	Allow backup of enterprise books	Determines whether the user can back up books distributed by the organization to iCloud or iTunes.	
	Allow in-app purchase	Determines whether the user can make in-app purchases.	
	Allow managed apps to store data in iCloud	Determines whether managed app data should sync with iCloud.	
	Allow notes and highlights sync for enterprise books	Determines whether metadata, which includes notes and highlights of books that are distributed by the user's organization, should be synced with iCloud.	
	Allow News	Determines whether the user can access News apps.	iOS 9.0+
	Allow System App Removal	Determines whether the user can remove system apps from the device.	iOS 11.0+
Network	Allow cellular plan modification	Determines whether users can modify the cellular plan.	iOS 11.0+
	Allow eSIM modifications	Determines whether users can modify the cellular plan for the eSIM card that is embedded in the device.	iOS 12.1+

Tab	Settings	Description	Applicable from
	Allow Bluetooth setting modification	Determines whether the user can modify the bluetooth settings on the device.	iOS 10+
	Allow personal hotspot modification	Determines whether users can modify the personal hotspot settings.	iOS 12.2+
	Allow Wi-Fi whitelisting	Determines whether or not the user can connect to the Wi-Fi service that is setup using the configuration profile.	iOS 10.3+
	Force Wi-Fi power on	Determines whether the user can turn off the Wi-Fi on the device from Settings menu or the Control Center even during airplane mode. This setting does not prevent the user from selecting which Wi-Fi network to use on the device.	iOS 13+
Apple Watch	Force Apple Watch wrist detection	Determines whether an Apple Watch should display the time and the latest alerts when the user's wrist is raised.	iOS 8.2+
	Allow pairing with Apple Watch	Determines whether the user can pair with an Apple Watch.	iOS 9.0+
iTunes	Allow iTunes	Determines whether the user can access the iTunes music store app.If disabled, the icon will be removed from the Home screen.	
	Require iTunes Store password for each purchases	Determines whether or not the user needs to enter the password for each purchase on the iTunes Store.	iOS 5.0+
iCloud	Allow My Photo Stream	Determines whether a copy of any photo taken on the managed device should be synced with the user's other iOS or iPadOS devices.	iOS 6.0+

Tab	Settings	Description	Applicable from
	Allow iCloud Keychain	Determines whether Keychain data such as accounts, passwords, and credit card information, should be synced with iCloud.	iOS 7.0+ and macOS 10.12+
	Allow iCloud Photo Library	Determines whether photos on iCloud can be accessed on the managed device. If disabled, any photos that are not fully downloaded from the Photo Library to the device, will be removed from local storage.	iOS 9.0+ and macOS 10.12+
	Allow iCloud Photo Sharing	Determines whether the user can publish and share photos with other iOS or iPadOS users through the iCloud website.	
	Allow iCloud backup	Determines whether data can be backed up or restored on iCloud.	iOS 5.0+
	Allow iCloud document sync	Determines whether the user can synchronize documents and key-values to the iCloud storage space.	iOS 5.0+ and macOS 10.11+
Safari	Allow use of Safari	Determines whether the user is allowed to use the Safari web browser on the device. If set to **No**, then the Safari icon is removed from the Home screen of the device.	

Tab	Settings	Description	Applicable from
	Accept cookies	Determines the cookie policy that should be enabled in the Safari web browser. The accepted values are: ◆ Block all websites, third parties, and advertisers from storing cookies on the device. ◆ Allow all websites, third parties, and advertisers to store cookies on the device. ◆ Allow cookies to be stored from only those websites that the user is currently visiting and not from third parties that embed content in the website. ◆ Allow cookies to be stored from only those websites that the user visits. With this option you can prevent websites that have embedded content in other websites that you visit from storing cookies. The default value is to allow cookies from all websites, third parties, and advertisers.	
	Allow pop-ups	Determines whether pop-ups should be blocked in the Safari web browser. This setting is enabled, if **Allow use of Safari** is configured as **Yes** or **Inherit**.	
	Enable autoFill	Determines whether Safari should remember the data entered by users on web entry forms. This setting is enabled, if **Allow use of Safari** is configured as **Yes** or **Inherit**.	

Tab	Settings	Description	Applicable from
	Enable JavaScript	Determines whether JavaScript should be enabled in the Safari web browser. This setting is enabled, if **Allow use of Safari** is configured as **Yes** or **Inherit**.	
	Force fraud warning	Determines whether Safari should warn users about refraining from visiting websites that are fraudulent. This setting is enabled, if **Allow use of Safari** is configured as **Yes** or **Inherit**.	
Lock Screen	Allow passbook notifications in lock screen	Determines whether notifications on the passbook app can be displayed on the lock screen. The passbook app allows users to store their coupons, tickets, and so on.	iOS 6.0+
	Allow voice dialing while device is locked	Determines whether voice dialing should be enabled while the device is locked.	
	Show Control Center in lock screen	Determines whether Control Center can be accessed from the Lock screen. The Control Center gives the user quick access to the apps and controls on the device.	iOS 7.0+
	Show Notification Center in lock screen	Determines whether users can view past notifications on the lock screen. If enabled, the users can still view notifications on the lock screen, when they arrive.	iOS 7.0+
	Show Today View in lock screen	Determines whether the Today View in Notification Center should be displayed on Lock screen.	iOS 7.0+
	Allow USB connections when device is locked	Determines whether the device can connect to USB accessories while locked.	iOS 12.0+

Tab	Settings	Description	Applicable from
Media Content	Allow bookstore erotica	Determines whether the user is permitted to download media that is tagged as erotica from the iBooks store.	iOS and tvOS 11.3+
	Allow explicit content	Determines whether the user can access explicit music or video content purchased from the iTunes Store. Explicit content is marked by the content providers when sold in the iTunes Store.	iOS and tvOS 11.3+
	Ratings region	Determines the region that needs to be selected to populate the allowed ratings for media content defined for that region.	iOS and tvOS 11.3+
	Apps	Determines the maximum allowed rating for apps. These values are populated based on the selected **Ratings region**. If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded or installed on the device.	iOS 5.0+ and tvOS 11.3+
	Movies	Determines the maximum allowed rating for movies. The values in this field are populated based on the selected **Ratings region**. If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded on the device.	iOS and tvOS 11.3+
	TV Shows	Determines the maximum allowed rating for TV shows. The values in this field are populated based on the selected **Ratings region**. If a rating is enabled, items that do not conform to the rating restrictions cannot be downloaded on the device.	iOS and tvOS 11.3+

Tab	Settings	Description	Applicable from
Security	Allow Touch ID to unlock device	Determines whether the user can unlock the device by using fingerprint.	iOS 7+ and macOS 10.12.4+
	Allow passcode modification	Determines whether the user can modify the passcode on the device. If disabled, the user will not be able to add, change or remove the passcode. Applicable for supervised devices only. This restriction is ignored in shared iPads.	iOS 9.0+
	Allow Touch ID fingerprint modification	Determines whether the user can modify the Touch ID fingerprints. This field will be enabled if the **Allow passcode modification** option is enabled.	
	Force authentication before using autofill	Determines whether users need to authenticate using Touch ID or Face ID before entering passwords or credit card information in Safari and Apps.	iOS 12.0+
	Allow password autofill	Determines whether users can use the Autofill Passwords feature and will be prompted to use saved passwords in Safari or in apps. If disabled, Automatic Strong Password will not be applicable and strong passwords will not be suggested to users.	iOS 12.0+
	Allow password sharing	Determines whether users can share their passwords using the Airdrop Passwords feature.	iOS 12.0+
	Allow password proximity request	Determines whether the device can request passwords from nearby devices.	iOS 12.0+
Gaming	Allow Game Center	Determines whether the user can access the Game Center. If disabled, the Game Center icon is removed from the Home screen.	iOS 6.0+

Tab	Settings	Description	Applicable from
	Allow multiplayer Gaming	Determines whether games with more than one player is enabled. This field will be enabled if the **Allow Game Center** option is enabled.	
	Allow adding Game Center friends	Determines whether game center friends can be added. This field will be enabled if the **Allow Game Center** option is enabled.	
Keyboard	Allow predictive keyboard	Determines whether the user can use predictive keyboard on the device.	iOS 8.1.3+
	Allow keyboard shortcuts	Determines whether the user can use shortcuts from external keyboards.	iOS 9.0+
	Allow auto correction	Determines whether users can use the auto correct option and select appropriate words.	iOS 8.1.3+
	Allow spell check	Determines whether spell check is allowed on a user's device.	iOS 8.1.3+
	Allow QuickPath keyboard	Determines whether the user can use the QuickPath keyboard.	iOS 13+
Music	Allow Music service	Determines whether Music Service is enabled on the device. If No is selected, then the Music Service is disabled and set to the classic mode.	iOS 9.3+ and macOS 10.12+
	Allow Radio	Determines whether the user can access iTunes Radio.	iOS 9.0+
	Allow Podcasts	Determines whether the user can access iTunes Podcasts.	iOS 8.0+
AirPrint	Allow AirPrint	Determines whether or not a user can connect to the AirPrint feature to print documents or pictures wirelessly using any AirPrint enabled printer.	iOS 11.0+

Tab	Settings	Description	Applicable from
	Allow AirPrint Credentials Storage	Determines whether or not AirPrint credentials can be stored in Keychain.	iOS 11.0+
	Force AirPrint Trusted TLS Requirement	Determines whether or not devices can connect to AirPrint enabled devices only using the trusted TLS certificates.	iOS 11.0+
	Allow AirPrint iBeacon Discovery	Determines whether or not devices can discover the printer beacons. Using these ibeacons, printers can broadcast connection information, and devices can discover it to reduce setup time.	iOS 11.0+
OS Update	Allow delay in OS updates	Determines whether user visibility of software updates should be delayed.	iOS 12.0+
	Select number of days for delay	Select for how many days the software update should be delayed, after which the software update is visible to the user. The maximum number of days is 90 days and the default value is 30 days.	iOS 12.0+
Classroom App	Force users to automatically join Classroom	Determines whether permission to join classes is automatically granted without prompting the student.	iOS 12.0+
	Allow teacher to lock apps and devices	Determines whether a teacher can lock apps or the entire device without prompting the student.	iOS 12.0+
	Force request for teacher consent before leaving Classroom	Determines whether a student enrolled in an unmanaged course needs to request for permission before leaving the course.	iOS 12.0+

Tab	Settings	Description	Applicable from
	Allow teacher to observe device screen	Determines whether the device of a student enrolled in a managed course, can automatically give permission to that course's teacher's request to observe the student's device screen, without prompting the student.	iOS 12.0+
Find My	Allow Find My Device	Determines whether the Find My Device feature in the Find My app can be enabled or not.	iOS 13+
	Allow Find My Friends	Determines whether the Find My Device feature in the Find My app can be enabled or not.	iOS 13+
	Allow Find My Friends setting modification	Determines whether the user can modify the Find my Friend settings on the device.	
Files	Files app - Allow network drive access	Determines whether the user can connect to the network drive in the Files app.	iOS 13.1+
	Files app - Allow USB drive access	Determines whether the user can access the USB drive in the Files app.	iOS 13.1+

Android Devices

The settings that can be enabled or disabled for Android devices are as follows:

	Settings	Description	Applicable from
Devices	Allow camera	Determines whether the device camera should be enabled. If disabled on devices enrolled in the work profile mode, the camera can still be accessed from the device's personal space.	Android 5.0+
	Allow install from unknown sources	Determines whether or not the user can install apps from outside the managed Google Play Store.	Android 5.0+
	Allow debugging features	Determines whether or not debugging of the device can be enabled.	Android 5.0+

Settings	Description	Applicable from
Allow screenshots	Determines whether the user can capture images of the device's display screen.	Android 5.0+
Allow cross-profile copy and paste	Determines whether the user can copy and paste data between the work profile and the personal space on the device.	Android 7.0+
Allow user to factory reset the device	Determines whether the user can factory reset the device from the settings menu of the device.	Android 5.1+
Allow factory reset protection	Determines whether devices need to be protected from an unauthorized (hard) factory reset. If enabled, this setting provides the ability to whitelist one ore more corporate unlock accounts which can be used to provision devices after unauthorized factory resets such as from bootloader or fast boot.	Android 5.1+
Specify corporate unlock accounts	This setting is enabled if **Allow factory reset protection** is enabled. Specify the corporate accounts of users who are authorized to provision devices that have undergone a hard factory reset.	Android 5.1+
Allow mounting of physical external media	Determines whether the user can connect their devices to external physical media.	Android 5.1+
Allow sharing data using NFC beam	Determines whether the user can share data from their devices using the NFC beam.	Android 5.1+
Allow USB file transfer	Determines whether the user can transfer files over USB.	Android 5.1+
Allow USB storage	Determines whether USB storage is enabled or disabled.	Android 5.1+
Allow cross-profile contact search	Determines whether the telephony or messaging apps in the personal space of a device can access work profile contacts.	Android 7.0+
Allow cross-profile caller ID lookup	Determines whether caller ID information of work profile contacts should be displayed in the personal space of a device during incoming calls.	Android 7.0+
Allow contact sharing with other bluetooth devices	Determines whether the user can share work contacts to other connected bluetooth devices such as hands-free calling in cars or headsets.	Android 7.0+

	Settings	Description	Applicable from
	Allow location configuration	Determines whether the user can turn the location on or off. If disabled, the user will not be able to turn on the Location setting on the device and you will not be able to determine the location of the device.	Android 9.0+
	Set location services mode	Set the location services mode to any one of the following to estimate the device location faster and more accurately: ◆ **High Accuracy** uses GPS, Wi-Fi, mobile network and sensors to determine the most accurate location. ◆ **Battery saving** uses sources that use less battery, like Wi-Fi and mobile networks. ◆ **Sensor only** uses only GPS (not including network-provided location). This mode consumes more battery and takes time in determining location.	Android 5.0+
	Allow Printing	Determines whether users can print data from their devices.	Android 9.0+
	Allow data sharing from personal to work profile	Determines whether users can share data from the personal profile to the work profile. If enabled, users can share data from apps in the personal profile to work profile apps. Also, work profile apps can pick items from the personal profile, such as files or pictures.	Android 9.0+
Apps	Runtime permissions	Select the default response for any runtime permissions requested by apps. For more information, see the Android Developer Documentation (https://developer.android.com/training/permissions/requesting.html). You can select any one of the following values: ◆ Prompt: Allows the user to grant or deny permissions to the apps. ◆ Auto Grant: Automatically grant permissions to the apps. ◆ Auto Deny: Automatically denies permission to the apps.	Android 6.0+

	Settings	Description	Applicable from
	Allow adding accounts	Determines whether the user can add or remove accounts to access work apps. However, this setting should be used with caution, as by enabling it users can also add their personal accounts to access work apps, which might make it difficult to contain corporate data within the workspace.	Android 5.0+
	Allow public play store access	Determines whether the user can access play store using the newly added account. This field will be enabled, if the **Allow adding accounts** field is enabled.	
	Allow Verify Apps enforcement	Determines whether Verify Apps can be enabled on the device. This feature scans apps for malware before and after the apps are installed, thereby securing corporate data from malicious apps.	Android 5.0+
	Allow apps to be uninstalled	Determines whether users can uninstall apps.	Android 5.0+
	Allow modifying of app data	Determines whether users can modify app data from the Settings menu such as uninstalling of apps, disabling of apps, clearing of app data and cache, force stopping apps, clearing app defaults and so on.	Android 5.0+
Network	Allow cell broadcasts	Determines whether users can configure cell broadcasts.	Android 7.0+
	Allow editing of mobile network settings	Determines whether users can modify the mobile network settings from the Settings menu.	Android 7.0+
	Allow resetting of all network settings	Determines whether users can reset network settings such as current cellular and Wi-Fi settings, VPN settings and so on.	Android 7.0+
	Allow cellular data while roaming	Determines whether device permits cellular data while roaming.	Android 7.0+
	Allow outgoing calls	Determines whether the users can make calls on their devices.	Android 7.0+
	Allow sending and receiving of SMS messages	Determines whether the device can receive text messages or whether users can send text messages.	Android 7.0+

	Settings	Description	Applicable from
	Allow tethering and configuring portable hotspots	Determines whether users can use their device as a portable hotspot by tethering.	Android 7.0+
	Set Wi-Fi timeout	Determines whether the device should disconnect from the connected Wi-Fi network, when the device is not in use. If the **Not when plugged in** option is selected, then the Wi-Fi will not timeout if the device is plugged-in.	Android 7.0+
	Allow bluetooth configuration	Determines whether users can configure bluetooth on their devices.	Android 7.0+
	Allow editing of ZENworks-provisioned Wi-Fi settings	Determines whether the user can modify the Wi-Fi settings that are provisioned by ZENworks.	Android 6.0+
	Allow changing of Wi-Fi network	Determines whether the user can connect to different Wi-Fi access points.	Android 6.0+
	Allow airplane mode	Determines whether users can set their devices in the airplane mode.	Android 9.0+
Audio	Mute master volume	Determines whether the master volume is remotely muted or not.	Android 5.0+
	Allow editing of volume settings	Determines whether users can modify the device volume settings.	Android 5.0+
	Allow muting of device microphone	Determines whether users can mute the device microphone.	Android 5.0+
Date	Allow configuration of date, time and time zone	Determines whether the user can configure the date, time and timezone settings, either manually or automatically.	Android 9.0+
	Allow configuration of date and time	Determines whether the users can configure the date and time on their devices either automatically or manually. If disabled, the date and time settings are disabled.	Android 5.0+
	Allow automatic update of date and time	Determines whether the date and time should be automatically fetched from the network. If enabled, the user will not be able to set the date and time manually.	Android 5.0+

	Settings	Description	Applicable from
	Allow automatic update of time zone	Determines whether the time zone should be automatically fetched from the network. If enabled, the user will not be able to set the time zone manually.	Android 5.0+
OS Update	Select OS update type	Select from any one of the following options to configure and apply over-the-air system updates for devices: ◆ Automatic indicates that the devices will receive the update as soon as it is available. ◆ Postpone indicates that the update can be postponed to up to 30 days. ◆ Windowed indicates that the update can be scheduled within a daily maintenance window. You can set the start time and the end time (based on a 24 hour format) in the **Daily maintenance window start time** and **Daily maintenance window end time**, respectively. The system update will install at any time between the start and the end time. If the start time is later than the end time, then the end time will be considered as a time on the next day.	Android 6.0+
Keyguard Features	Allow device keyguard features	Determines whether features such as Trust Agents and Fingerprint Unlock are made available to users before unlocking the device lock screen.	Android 5.0+
	Allow trust agents	Determines whether trust agents such as Smart Lock can be enabled by the user to unlock the device keyguard. If you select **Configure**, then you can enable or disable specific Google Smart Lock trustlets in the **Smart Lock** field. If you select **All,** then all the Trust Agents will be automatically enabled for the user to configure on the device.	Android 5.0+

	Settings	Description	Applicable from
	Smart Lock	The Smart Lock feature lets users keep their Android devices unlocked when any of the following options are enabled: ◆ **Bluetooth:** When enabled, this option lets the user add a bluetooth device such as a bluetooth watch to the Trusted Devices setting on the device. The user's device remains unlocked as long as it is connected to one of these trusted devices. ◆ **NFC:** When enabled, this option lets the user add an NFC device to the Trusted Devices setting on the device. The user's device remains unlocked based on the NFC tags on the trusted devices. ◆ **Places:** When enabled, this option lets the user add a safe location such as the user's home or office, in the Trusted Places setting. The user's device unlocks and remains unlocked as long as the current location of the user is one of the configured Trusted Places. ◆ **Faces:** When enabled, this option lets the user set his or her face as a Trusted Face. The user's device unlocks when it recognizes the user's face. ◆ **On Body:** When enabled, this option lets the user configure On Body Detection on the device. Based on this setting, the device will unlock and will remain unlocked until it is being carried in the user's hand, bag, or pocket, which is detected based on the device's motion sensors such as the accelerometer or gyroscope. ◆ **Voice:** This option enables the device to unlock when the user uses the voice command "OK Google".	Android 5.0+
	Allow fingerprint unlock	Determines whether users can unlock their devices using their fingerprints.	Android 5.0+

	Settings	Description	Applicable from
	Allow redacted notifications	Determines whether the user can enable all notifications, including redacted (containing sensitive information) notifications, on the lock screen. If disabled, the user has the option to disable redacted notifications on the lock screen.	Android 5.0+
	Allow secure camera	Determines whether the camera can be accessed from the lock screen.	Android 5.0+
	Allow all notifications	Determines whether all notifications are displayed on the lock screen.	Android 5.0+
Display	Allow ambient display	Determines whether the user can configure ambient display on their devices.	Android 9.0+
	Allow screen brightness	Determines whether the users can configure screen brightness on their devices.	Android 9.0+
	Set screen brightness mode	Determines whether the screen brightness mode should be set to automatic.	Android 9.0+
	Configure screen brightness percentage	Determines whether a specific backlight brightness percentage should be enforced. If enabled, you can set the percentage in the **Set Brightness Percentage** field. The brightness value on an Android device ranges from 0 to 255. When you define a percentage in the **Set Brightness Percentage** field, then the equivalent value is set on the device. For example, if 50% is set as the brightness percentage, then the brightness value is set as 127.5.	Android 9.0+
	Allow user to configure screen timeout	Determines whether the user can configure when the device screen should timeout.	Android 9.0+

ActiveSync Devices

These settings can be applied on devices that are enrolled as:

- ActiveSync Only devices
- Fully Managed iOS and ActiveSync (iOS MDM + ActiveSync) devices.

If a setting is applicable for both iOS and Activesync, then the stricter restriction of the two is applied. For example, if **Allow Camera** is enabled as a part of the iOS settings and if **Allow Camera** is disabled as a part of the ActiveSync settings, then the camera icon is removed from the device, as disabling of the camera is a strict setting.

Settings	Description
Allow Bluetooth	Determines whether bluetooth connections are allowed to and from the device. You also have the option of allowing only a hands free configuration on the device.
Allow browser	Determines whether the user is allowed to use the default web browser on the device.
Allow camera	Determines whether the device camera should be enabled.
Allow infrared	Determines whether infrared connections are allowed to and from the device.
Allow text messaging	Determines whether the user can send or receive text messages on the device.
Allow storage card	Determines whether the device can access a removable storage card.

Doc Updates

In the 2020 Update 1 release, the following changes are made:

Introduction of new tabs for Apple Devices: Three new tabs Network, Find My, and Files have been introduced in this release, which contain new settings for Apple devices. Also, the following existing settings have been moved to these tabs:

Bluetooth setting modification is moved to the Network tab.

Allow Find My Friends setting modification is moved to the Find My tab.

Allow Wi-Fi whitelisting is moved to the Network tab.

Introduction of new settings for Apple devices in the existing tabs: The Allow UI configuration profile installation and Allow QuickPath keyboard settings have been introduced in the Device and Keyboard tabs, respectively.

Legal Notices