Agent settings: Mobile Security

Tools > Configuration > Agent settings > Mobility Legacy > Mobile Security

The Mobile Security dialog box allows you to configure security settings on mobile devices.

The General page allows you to provide a name for the settings and set it as the default setting.

If you disable options after the settings have been distributed to devices, the settings are removed from devices. If you disable a passcode requirement, the requirement is removed from the device, but the passcode is not.

Passcode page

The passcode settings here are applied to selected Android, iOS, OS X, and Windows 10/11 devices. This page contains the following options:

- **Enable passcode settings:** Allows you to configure settings for increased security in accessing devices.
- **Minimum password quality:** A **Simple** password would be something easily guessed, such as 1111 or ABCD. If you set the minimum password quality to **Alphanumeric**, the password must contain at least one letter and at least one number.
- **Minimum password length:** Set a minimum length for the password.
- **Lock screen after:** The length of time in minutes of inactivity before the screen locks.
- **Maximum number of failed password attempts before device wipe:** The number of failed attempts to unlock the device before all data on the device is erased.

iOS Restrictions page

The iOS restriction options allow you control over how the device is used. Some options are only available if the device is in Supervised mode. For information about putting a device into Supervised mode, see your Apple documentation.

This page contains the following options:

- **Enable iOS restrictions settings:** Applies the settings on the Device Functionality, Application, Single-app mode, iCloud, and Security and Privacy pages.

Device Functionality page

- **Allow installing apps:** Allows the user to install apps. Removing the check for this option does not prevent users from deleting apps on the device. Modern Device Management cannot prevent the removal of apps at the device level.
- **Allow use of camera:** Allow the user to launch the camera application.

- **Allow FaceTime:** Allows the user to place or receive FaceTime calls.
- **Allow screen capture:** Allows the user to save a screen-shot of the display.
- **Allow automatic sync while roaming:** Allows the device to sync accounts automatically even when the device is roaming.
- **Allow Siri:** Allows the user to use Siri, voice commands, or dictation.
- **Allow Siri while locked:** Allows the user to use Siri without entering a passcode when the device is locked.
- **Allow Siri querying user-generated content (Supervised only):** Allows access to content in Siri added by other users.
- **Allow voice dialing:** Allows the user to dial using a voice command.
- **Allow Passbook while device is locked:** Allows the device to display Passbook notifications while the device is locked.
- **Allow in-app purchases:** Allows the user to make purchases through installed apps.
- **Force user to enter password for all purchases:** Forces the user to type in his iTunes Store account password each time he makes a purchase.
- **Allow multiplayer gaming:** Allows the user to play multiplayer games in the Game Center.
- **Allow adding Game Center friends:** Allows the user to add friends in the Game Center.
- **Allow Control Center while locked:** Allows the user to swipe up to view the Control Center even when the device is locked.
- **Allow Notification view while locked:** Allows the user to view notifications even when the device is locked.
- **Allow Today view while locked:** Allows the user to swipe down to see the Today View even when the device is locked.
- **Allow iBooks Store:** Allows the user to access the iBooks Store. This option is only applied if the device is in Supervised mode.
- **Allow use of AirDrop:** Allows the user to access AirDrop. This option is only applied if the device is in Supervised mode.
- **Allow account change:** Allows the user to change account settings. This option is only applied if the device is in Supervised mode.
- **Allow cellular data usage for apps:** Allows apps on the device to use a cellular data connection. This option is only applied if the device is in Supervised mode.

Applications page

- **Allow use of iTunes Store:** Allows the user to access the iTunes Store.
- **Allow Web browser:** Allows the user to launch Safari. When this option is disabled, the user cannot launch Safari, but is still able to launch other Web browsers, such as Chrome.
- **Enable autofill:** Allows the user to turn on Safari's autofill feature.
- **Limit AD tracking:** Prevents the device's ID from being used for advertisement tracking.
- **Force fraud warning:** When the user visits a fraudulent or compromised web site, Safari displays a warning.
- **Allow JavaScript:** Allows web pages that the user accesses using Safari to run JavaScript.
- **Block pop-ups:** Sets Safari to block pop-up messages.
- **Accept cookies:** Allows Safari to accept all cookies, reject all cookies, or accept cookies only from sites that are directly accessed.
- **Allow change to FindMyFriends (Supervised only):** Allows apps to access Find My Friends.

Content and Ratings page

- **Allow explicit content:** Limits the device to only run content meeting the rating standard specified for that content type.
- **Sets the region for the ratings:** Determines the national standards to use for defining explicit content.
- **Movies:** Specifies the maximum rating allowed for movie content to play on the device.
- **TV Shows:** Specifies the maximum rating allowed for TV show content to play on the device.
- **Apps:** Specifies the maximum rating allowed for Apps to install and launch on the device.

Single-app mode (Kiosk)

- **Enable kiosk mode:**Also known as guided access, this option limits the device to only run the app specified. When kiosk mode is enabled, the device will only launch the app specified and will block other apps. To specify the app for kiosk mode, use the Apple ID. To exit kiosk mode, an administrator must modify the agent settings to turn off kiosk mode and update the device. Kiosk mode is only available for devices that are in Supervised mode. For more information, see your Apple documentation.
- **Apple ID of application to run:** The Apple ID of the application that is allowed to run in kiosk mode.
- **Disable Autolock:** Prevents the device from locking automatically.
- **Disable device rotation:** Disables the display from changing orientation when the device is rotated.
- **Disable ringer switch:** Disables any functionality associated with the ringer switch.

- **Disable sleep/wake button:** Disables any functionality associated with the sleep/wake button.
- **Disable touch:** Disables the touch functionality of the screen.
- **Disable volume button:** Disables any functionality of the volume button.
- **Allow Assistive Touch:** Allows the user to use Assistive Touch features to make the device more accessible. This option is for users who have problems touching the screen or pressing buttons.
- **Allow Assistive Touch adjustment:** Allows the user to configure Assistive Touch options.
- **Allow invert colors:** Allows the user to invert the colors on the screen.
- **Allow user to adjust color inverting:** Allows the user to configure color inversion options.
- **Allow mono audio:** Allows the user to switch the audio output to mono.
- **Allow Speak Selection:** Allows the user to select text and use the Speak Selection feature for text-to-speech.
- **Allow VoiceOver:** Allows the user to use VoiceOver features to make the device more accessible. This option is for users who need audible presentation of screen materials or menus.
- **Allow user to adjust VoiceOver:** Allows the user to configure VoiceOver options.
- **Allow zoom:** Allows the user to use zoom features.
- **Allow user to change zoom:** Allows the user to change the zoom settings.
- **Autonomous permitted App IDs to run:** Allows apps identified by the bundle IDs to enter Single App Mode. This option only applies if you have apps that have the ability to enter Single App Mode. Modern Device Management does not make apps enter Single App Mode, it only allows the app to do it.

iCloud page

- **Allow backup:** Allows the user to back up the device using iCloud.
- **Allow document sync:** Allows the user to store documents in iCloud.
- **Allow Photo Stream:** Allows the user to use Photo Stream. If Photo Stream is disabled after the device user has shared photos using Photo Stream, photos already shared are removed.
- **Allow shared photo streams:** Allows the user to share his photo stream and view others' photo streams.

Security and Privacy page

- **Allow unlocking by Touch ID:** Allows the user to use Touch ID to unlock the device.
- **Allow Host Pairing (Supervised only):** Allows the device to pair with computers other than the computer used to put the device in Supervised mode.

- **Allow diagnostic data to be sent to Apple:** Allows the device to send diagnostic data to Apple.
- **Allow user to accept untrusted certificates:** Allows the user to accept TLS certificates that can't be verified. This setting is enforced for Safari, Mail, Contacts, and Calendar.
- **Allow open from managed to unmanaged Apps/Accounts:** Allows the user to switch to unmanaged applications or accounts from a managed app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link in an email that launches the browser.
- **Allow open from unmanaged to managed Apps/Accounts:** Allows the user to switch to managed apps or accounts from an unmanaged app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link on a web page that launches the email app.
- **Allow Over-The-Air PKI updates:** Allows public key infrastructure updates. If this option is not enabled, the user may experience issues with any application that depends on certificates, including Internet browsers.
- **Allow interaction while install config profile (Supervised only):** Allows the administrator to send down configuration profiles silently, without user interaction.
- **Force encrypted backups:** Forces the user to encrypt any backups using iTunes.

Android Restrictions page

The Android restriction options allow you control over how the device is used. Certain settings only apply to specific profiles, such as those related to Android for Work.

This page contains the following options:

- **Enable Android restrictions settings:** Applies the settings on the Device Functionality, Application, and App Lists pages.

Device Functionality page

Standard Mode tab

- **Allow use of camera:** Allows the user to launch the camera application.
- **Allow settings changes:** Allows the user to launch the settings app and alter configurations.
- **Allow Bluetooth:** Allows the user to activate Bluetooth and connect to wireless devices.

Profile Owner Mode tab

- **Allow installing apps:** Allows the user to install new apps on the device.
- **Allow use of camera:** Allows the user to launch the camera application.

- **Allow screen capture:** Allows the user to save a screenshot of the display.
- **Allow NFC:** Allows the user to use NFC functionality on the device.
- **Allow apps control:** Allows the user to manage apps on the device.
- **Allow config credentials:** Allows the user to alter credentials for accessing the device.
- **Allow cross-profile copy/paste:** Allows the user to copy and paste data between managed and non-managed apps.
- **Allow modify accounts:** Allows the user to modify individual user accounts on the device.
- **Allow share location:** Allows the user to share their device location with apps.
- **Allow uninstall apps:** Allows the user to remove apps from the device.

Device Owner Mode tab

- **Allow installing apps:** Allows the user to install new apps on the device.
- **Allow use of camera:** Allow the user to launch the camera application.
- **Allow screen capture:** Allows the user to save a screenshot of the display.
- **Allow settings changes:** Allows the user to launch the settings app and alter configurations.
- **Allow Bluetooth:** Allows the user to activate Bluetooth and connect to wireless devices.
- **Allow Microphone:** Allows the user to access the microphone.
- **Allow NFC:** Allows the user to use NFC functionality on the device.
- **Allow USB:** Allows the user to access device contents from a computer via a USB cable.
- **Allow USB Debug:** Allows the user to debug the device from a computer via a USB cable.
- **Allow Tethering (Bluetooth, Wi-Fi, USB):** Allows the user to tether peripheral devices to the Android device, such as Bluetooth headsets.
- **Allow add user:** Allows the user to add user accounts to the device.
- **Allow adjust volume:** Allows the user to change volume levels on the device.
- **Allow apps control:** Allows the user to manage apps on the device.
- **Allow config cell broadcasts:** Allows the user to configure broadcasts the device receives.
- **Allow config credentials:** Allows the user to alter credentials for accessing the device.
- **Allow config mobile networks:** Allows the user to alter mobile network settings.

- **Allow config vpn:** Allows the user to set up or alter VPNs on the device.
- **Allow config Wi-Fi:** Allows the user to configure Wi-Fi networks.
- **Allow create windows:** Allows the user to create windows.
- **Allow factory reset:** Allows the user to reset the device to its original factory state.
- **Allow install unknown sources:** Allows the user to install apps from unknown sources.
- **Allow modify accounts:** Allows the user to modify individual user accounts on the device.
- **Allow mount physical media:** Allows the user to mount physical external storage volumes.
- **Allow network reset:** Allows the user to reset all network settings.
- **Allow outgoing calls:** Allows the user to perform outgoing calls from the device.
- **Allow remove user:** Allows the user to remove individual user accounts from the device.
- **Allow safe boot:** Allows the user to boot the device using Safe mode.
- **Allow share location:** Allows the user to share their device location with apps.
- **Allow sms:** Allows the user to send SMS messages from the device.
- **Allow uninstall apps:** Allows the user to remove apps from the device.

Applications page

- **Allow Web applications:** Allows the user to launch the default Web browser. When this option is disabled, the user cannot launch that app, but is still able to launch other Web browsers.
- **Allow Mail applications:** Allows the user to access mail apps on the device.
- **Allow use of YouTube:** Allows the user to access the YouTube app.
- **Allow Play Store:** Allows the user to access the Play Store app.

App Lists page

- **Use App List:** Allows administrators to list specific applications that will be allowed or blocked on the device. Apps must be identified by name and package ID.
- **White List:** Allows administrators to globally restrict what apps can be installed or used on the device.
- **Black List:** Allows administrators to globally restrict what apps cannot be installed or used on the device.