How to setup restrictions for iOS devices via Endpoint Manager profile

Click ‘Configuration Templates’ > ‘Profiles’ > open an iOS profile > open the ‘Restrictions’ section

- The 'Restrictions' section of an iOS profile lets you define limitations for various user activities. Examples include use of camera, installing and uninstalling apps, connecting to Wi-Fi hot spots, in-app purchases, using iCloud backup and more.
- The activities are grouped under various categories, like Device Functionality, Security and Privacy, Content Ratings, Applications and iCloud.

Set restrictions in an iOS profile

- Device Functionality
- Security and Privacy
- Content Ratings
- Applications
- iCloud

Get App Identifier for iOS applications

Related topics

Set restrictions in an iOS profile

- Login to Comodo One / Dragon
- Click 'Applications' > 'Endpoint Manager'
- Click ‘Configuration Templates’ > ‘Profiles’
- Open the iOS profile applied to your target devices
    - Open the 'Restrictions' tab, if it has been added already, then click 'Edit'

      Or
    - Click 'Add Profile Section' > 'Restrictions', if it hasn't yet been added:

      The restrictions are grouped under the following categories. Click the links below for descriptions of the options under respective categories:

- Device Functionality
- Security and Privacy
- Content Ratings
- Applications
- iCloud

- Click 'Save' after configuring the options for your settings to take effect on the devices to which the profile Is applied.

Device Functionality

Allow installing apps - The user can install or update apps from the Apple App Store. If left unchecked, the 'App Store' icon is removed from the device's home screen.

Allow app uninstall - The user can uninstall applications from the device.

Allow use of the iMessage - The user can quickly and easily chat over iMessage or SMS/MMS.

Allow camera - The user can to take photos, videos or use FaceTime (if enabled). If left unchecked, the camera icon is removed from the device and camera is disabled.

Allow face time - The user can use FaceTime. Applies only if 'Allow Camera' is enabled.

Allow Personal Hotspot - The user can setup Wi-Fi hot-spots from their device and allow other devices to connect.

Allow screen shot - The user take screenshots on their device.

Allow global background fetch when roaming - Select this to allow various apps in the device to sync and fetch data from cloud when in roaming mode abroad.

Allow assistant - Users can use Siri voice commands and dictation.

Allow assistant while Locked - Users can use Siri even when the device is locked. Applies only if 'Allow Assistant' is enabled.

Allow assistant user generated content - Users can use Siri to query user-generated content from the internet or device.

Forces the use of the profanity filter assistant - Imposes profanity filter to Siri. The voice command, dictation and other Siri features are filtered accordingly.

Allow voice dialing – The user can dial their phone using voice commands, even if the phone is locked with a passcode.

Allow passbook while locked - Passbook notifications are shown even when the device is locked.

Allow in app purchases – The user can make in-app purchases, that is buying paid versions of apps, products or services, subscriptions and more, by tapping options in running applications, using real currency.

Force iTunes store password entry – The user needs to enter his/her iTunes password for every

transaction with Apple store.

Allow multiplayer gaming – User can play games with their friends in Game Center, an online multiplayer social gaming network

Allow adding Game Center friends - User can add friends to their Game Center account.

Allow account modification - User can add/remove accounts like Apple account, mail accounts and more, on the device. Applies only to iOS 7+ and supervised devices.

Allow air drop - User can use Air Drop to send and receive photos, documents, and more with other nearby Apple devices. Applies only to iOS 7+ and supervised devices.

Allow find my friends modification – User can use the Find My Friends feature to track locations of their friends, children and more. Applies only to iOS 7+ and supervised devices.

Allow fingerprint for unlock - Enable Touch ID to allow user to unlock his/her device using finger print. Applies only to iOS 7+ and supervised devices.

Allow Game Center - Users can access Game Center. Applies only to iOS 7+ and supervised devices.

Allow host pairing – Host pairing lets you control which devices the managed iOS device can pair with.

- **Enabled** - The device can pair with other computers and devices
- **Disabled** - The device cannot pair with any other device than the supervision device. If supervision host certificate has not been configured, the device cannot pair with a supervision device too.

Applies only to iOS 7+ and supervised devices.

Allow lock screen control center – Show 'Control Center' widget on the lock screen. Applies only to iOS 7+ and supervised devices.

Allow lock screen notifications view – Enable notifications history view on the lock screen, that allows user to view past notifications. If disabled, users will still be able to view notifications when they arrive. Applies only to iOS 7+ and supervised devices.

Allow lock screen today view - Show 'Today View' in Notification Center on the lock screen. Applies only to iOS 7+ and supervised devices.

Allow OTAPKI updates – Device can receive over-the-air public key infrastructure (OTAPKI) updates. The device can still perform certificate revocation list (CRL) and online certificate status protocol (OCSP) checks, even if this option is disabled. Applies only to iOS 7+ and supervised devices.

Allow UI configuration profile installation - User can locally install configuration profiles and certificates using the graphical user interface (UI) on the device. Applies only to iOS 7+ and supervised devices.

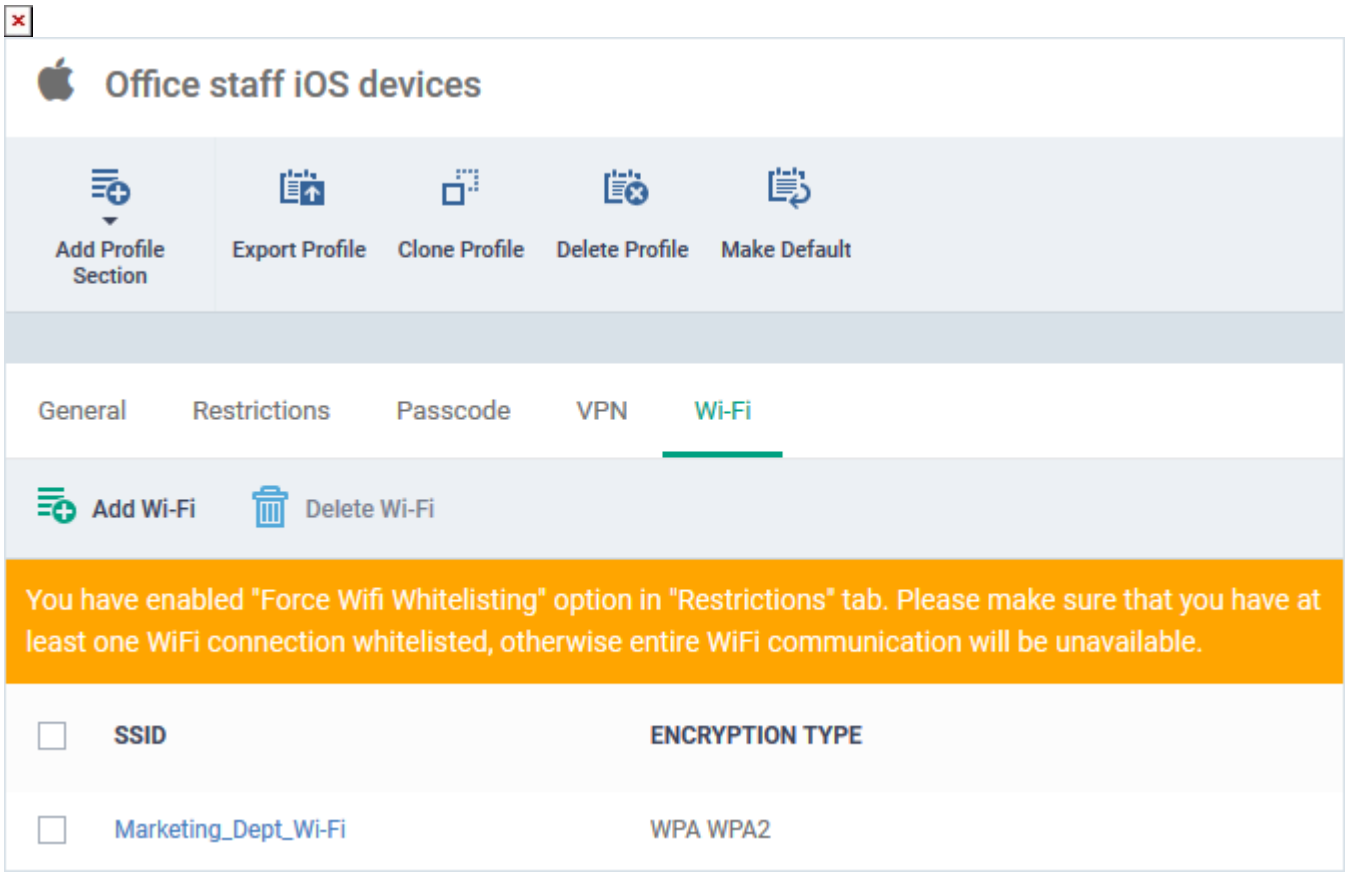
Force limit ad tracking - Prohibit users from ad tracking activities on the devices. Applies only to iOS 7+ devices.

Force Wifi Whitelisting – The device can connect only to the allowed Wi-Fi networks/hotspots, defined in the profile. Connection to any other Wi-Fi network is prohibited.

- You can add allowed Wi-Fi networks to the Wi-Fi section of the profile
- Click 'Configuration Templates' > 'Profiles' > click on the iOS profile > 'Add new section' > 'Wi-Fi'
- See How to specify allowed Wi-Fi networks for iOS devices for help to do this

- Please ensure at least one Wi-Fi network is added to the Wi-Fi section of the profile, if 'Force Wifi Whitelisting ' is enabled. Else the device will not be able to connect to any Wi-Fi networks.

- A notification is shown in the 'Wi-Fi' section of the profile if 'Force Wifi Whitelisting ' is enabled:



Forces all devices receiving AirPlay requests from this device to use a pairing password – User should enter a password for pairing while sending AirPlay requests to any other device.

Allow managed applications from using cloud sync - User can restrict managed apps backing up any data to iCloud, while still allowing it for user downloaded apps.

Allow the "Erase All Content And Settings" option in the Reset UI – Shows 'Erase All Content And Settings' option in the 'Reset' screen on the device. The user can choose to remove his/her personal information: credit or debit card, photos, contacts, music, or apps while resetting the device. Applies only to supervised devices.

Spotlight will return Internet search results - The 'Spotlight' feature on the device provides suggestions from the internet, iTunes, and the App Store for the user to quickly find any file, documents, emails, apps contacts and more on the device. Supervised devices only.

Allow the "Enable Restrictions" option in the Restrictions UI in Settings – Enables the 'Enable Restrictions' setting in the 'Restrictions' user interface of the 'Settings' screen. The user can configure various restriction settings and parental control from the 'Restrictions' interface. Applies to iOS 8+ and supervised devices only,

- For iOS 12 or later - If 'Restrictions' setting is replaced by 'ScreenTime'

Allow activity continuation – Enables the 'Handoff" feature on the device. The handoff feature enables user

to continue their on-going activities on different iOS devices in which they have signed-in with the same Apple account.

Allow backed up enterprise books - User can save iBooks to iCloud and control synchronization. Notes and highlights made to the enterprise books are synced to the backup.

Allow podcasts - User can receive their favourite podcasts. Applies only to supervised devices with iOS 8 and later versions.

Allow definition lookup - User can use spell check and dictionary lookup features on the device. Applies only to supervised devices with iOS 8 and later versions.

Allow predictive keyboard - Users can enable or disable the predictive keyboard feature. Applies only to supervised devices with iOS 8.1.3 and later versions.

Allow keyboard auto-correction - User can enable or disable auto-correct feature when typing. Applies only to supervised devices with iOS 8.1.3 and later versions.

Allow keyboard spell-check – User can enable/disable keyboard spell check feature. Applies only to supervised devices with iOS 8.1.3 and later versions.

Paired Apple Watch will be forced to use wrist detection - If an Apple Watch is paired with the device, the device forces the Apple Watch to enable Wrist Detection. Applies only to iOS 8.2 and later versions.

Allow music service and music - Lets third-party apps to add music to user's iCloud music library. Applies only to iOS 9.0 and later versions and supervised.

Allow iCloud Photo Library – User can use the iCloud Photo Library and upload photos and videos. Applies only to supervised devices with iOS 9 and later versions.

Allow News - User can subscribe to news services. Applies only to supervised devices with iOS 9.0 and later versions.

Causes AirDrop to be considered an unmanaged drop target - Airdrop on the device will be treated as an unmanaged destination for file transfers. Applies only to iOS 9.0 and later versions.

Enable the App Store on the home screen - Shows the AppStore icon on the home screen of the device.

Allow keyboard shortcuts - User can create and use keyboard shortcuts for typing snippets. Applies only to supervised devices with iOS 9.0 and later versions.

Allow pairing with an Apple Watch - User can pair the device with an Apple Watch. Applies only to supervised devices with iOS 9.0 and later versions.

Allow device passcode from being added, changed, or removed – User can create and modify screen lock passcodes for the device. Applies only to supervised devices with iOS 9.0 and later versions.

Allow device name modification – User can change the device name. Applies only to supervised devices with iOS 9.0 and later versions.

Allow wallpaper modification - User can change wallpapers displayed on the device. Applies only to supervised devices with iOS 9.0 and later versions.

Allow automatic download applications - Applications in the device can automatically download and install apps and updates. Applies only to supervised devices with iOS 9.0 and later versions.

Allow enterprise application trust - 'Trusted' status is automatically applied to enterprise applications. Applies only to devices with iOS 9.0 and later versions.

Allow enterprise application trust modification - Users can manually change the Trust status of enterprise applications. Applies only to supervised devices with iOS 9.0 and later versions.

Allow radio service - User can use Apple Music Radio on the device. Applies only to supervised devices with iOS 9.3 and later versions.

Allow notifications modification - User can modify 'Apple Push Notifications' settings on the device. Applies only to supervised devices with iOS 9.3 and later versions.

Whitelisted application bundles - Add applications to the app whitelist. The applications in the whitelist are skipped from security checks during installation and usage.

- Enter the App bundle ID of the application to be added to the whitelist.
- See the explanation at the end of this page for more details on obtaining the App bundle ID.
- Click the variables button to insert dynamic values. See this page for help to create and manage custom variables.
- Click the button to add more applications.
- Click the button to remove an app.

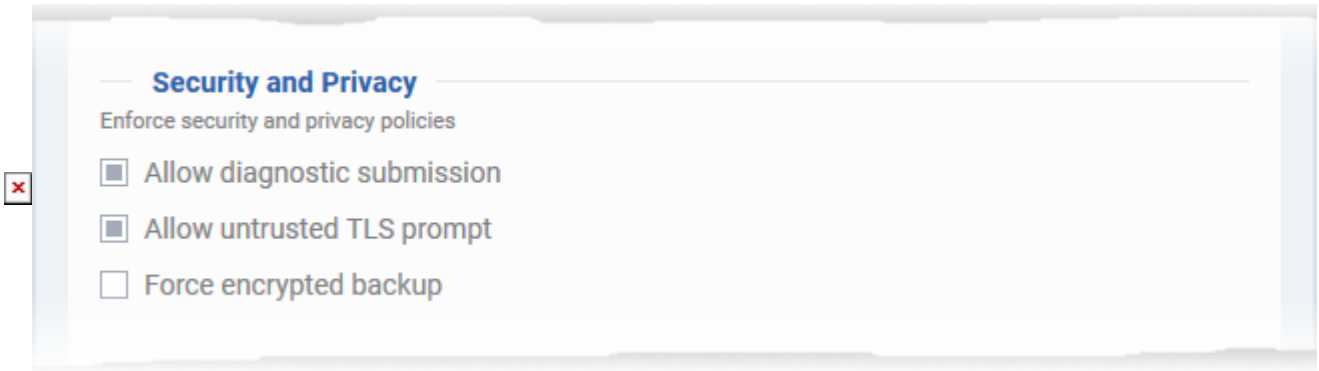
Note: This feature is available only for supervised devices with iOS 9.3 and later versions.

Blacklisted application bundles - Add applications to the app blacklist. The applications in the blacklist will not be allowed to be installed or used.

- Enter the App bundle ID of the application to be added to the blacklist.
- See the explanation at the end of this page for more details on obtaining the App bundle ID.
- Click the variables button to insert dynamic values. See this page for help to create and manage custom variables.
- Click the button to add more applications.
- Click the button to remove an app.

Note: This feature is available only for Supervised devices with iOS 9.3 and later versions.

Security and Privacy

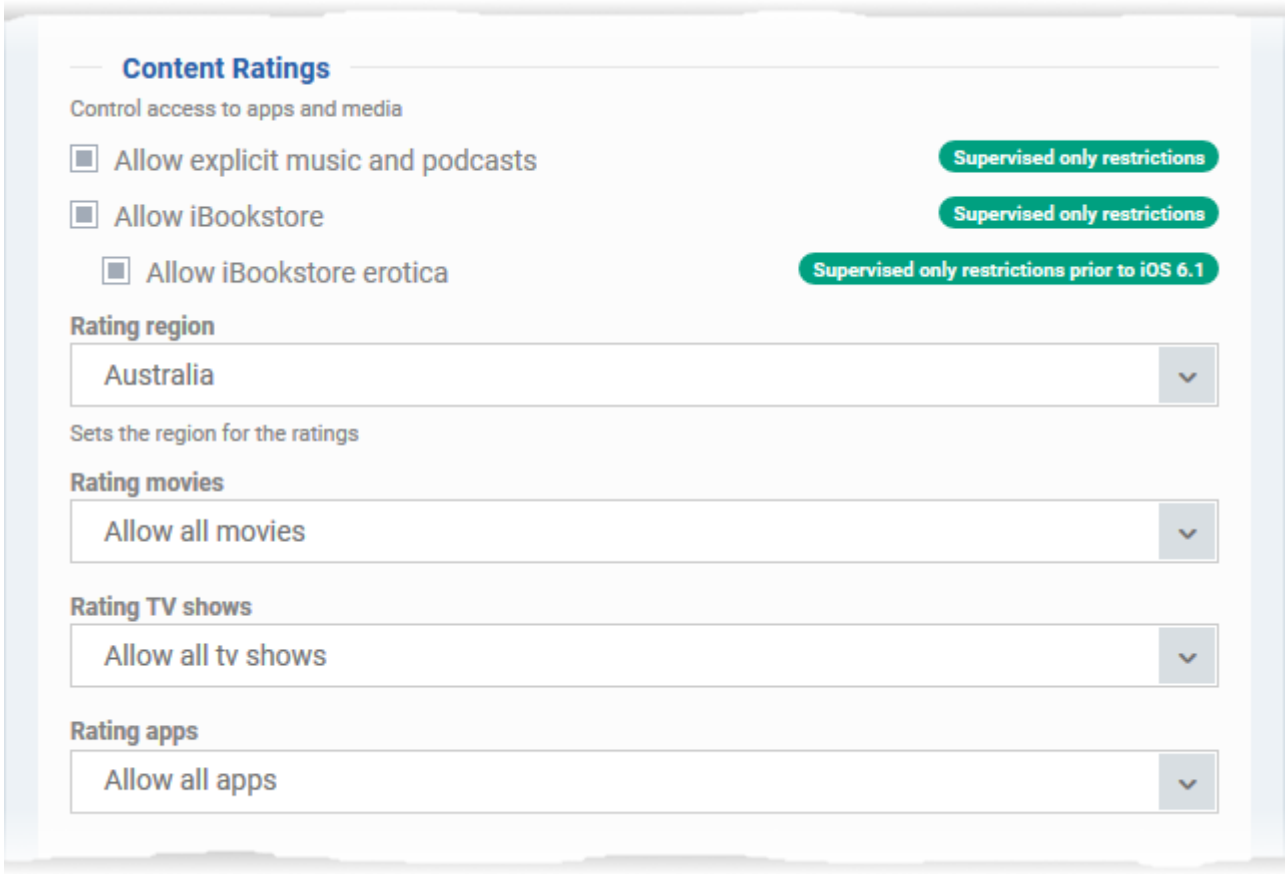


- **Allow diagnostic submission** - The device automatically submits diagnostic reports to Apple.

- **Allow untrusted TLS prompt** – The user will be prompted every time if they want to trust unverified certificates. This setting applies to Calendar accounts, Contacts, Safari and Mail.

- **Force encrypted backup** – All backup data from the device to iTunes will be automatically encrypted. If not enabled, the user can choose whether or not to encrypt the backup.

Content Ratings



Allow explicit music and podcasts - Content providers of iTunes flag their explicit content for easy identification.

- If enabled, explicit content including music and video will be shown in iTunes store instead of being hidden, on the device.

Allow iBookstore - User can access iBookstore, an online bookstore from Apple. Applies only to supervised devices.

Allow iBookstore erotica - User can download media tagged as erotica from iBooks. Applies only to supervised devices with versions prior to iOS 6.1.

Rating region - Select the region whose content ratings are to be followed, from the drop-down.

Rating movies - Choose the content rating to be allowed for watching movies.

Rating TV Shows - Choose the content rating to be allowed for watching the TV shows.

Rating apps - Choose the rating to be allowed for using apps.

Applications

Allow use of iTunes Store - Users can access iTunes store. If disabled, iTunes store will not be available on the device.

Allow Safari - Users can use Safari for browsing internet. If disabled, the Safari browser app will not be available on the device.

Allow auto fill - The 'auto-fill' feature is enabled for Safari, to automatically fill details such as user name, password, credit card details and so on in web forms.

Allow java script - Java script features are supported by Safari.

Allow popups - Popups are allowed in Safari.

Force fraud warning - Safari displays alerts to users when visiting websites that are identified as compromised or fraudulent.

Accept cookies - Select the option on when Safari can accept cookies, from the drop-down. The available options:

- Always
- Never
- From visited site

Allow app cellular data modification - User can modify cellular data usage settings for individual apps on the device. Applies only to supervised devices with iOS 7 or later versions.

Allow open from Managed to Unmanaged – Permits data transfer from managed apps to unmanaged apps. Applies only to iOS 7 and later versions.

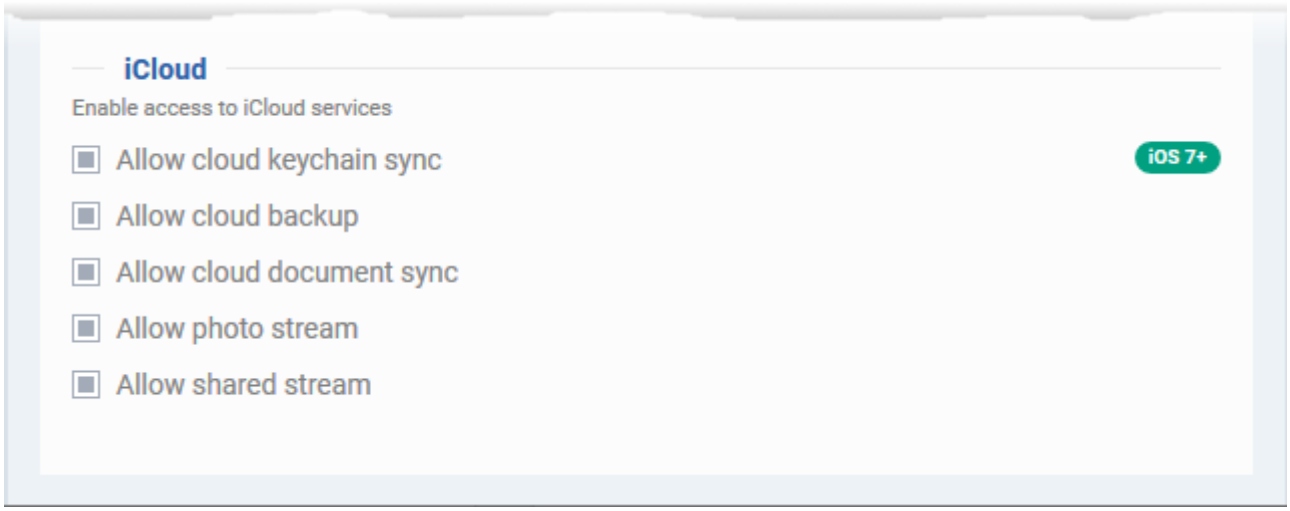
Allow open from Unmanaged to Managed – Permits data transfer from unmanaged apps to managed apps. Applies only to iOS 7 and later versions.

Autonomous single app mode permitted app bundle IDs - iOS apps built with the functionality of single App Lock, can provoke App Lock for them under certain scenarios in Autonomous single app mode.

- Specify the apps for which the mode can be enabled, by entering their App bundle IDs.
- See the explanation at the end of this page for more details on obtaining the App bundle ID.
- Click the variables button to insert dynamic values. See this page for help to create and manage custom variables.
- Click the  button to add more applications.
- Click the  button to remove a field.

Note: This feature applies only to supervised devices with iOS 7 or later versions.

iCloud



- **Allow cloud keychain sync** - The Apple Keychain data on the device will be periodically synced to iCloud. Applies only to iOS 7 and later versions.
- **Allow cloud backup** – User can backup their data on iCloud. Applies only to iOS 7 and later versions.
- **Allow cloud document sync** - User can synchronize documents on their device with iCloud. Applies only to iOS 7 and later versions.
- **Allow photo stream** - User can use the Photo Stream feature on the device. Applies only to iOS 7 and later versions.
- **Allow shared stream** - Users can share and view photos in Photo Stream. Applies only to iOS 7 and later versions.

Get App Identifier for iOS applications

App Store Application:

1. Find the iTunes Store download URL of the app. Example: https://itunes.apple.com/us/app/cmdm/id807480077?mt=8.

2. Copy the number after the id in the URL. (Here it is: 807480077).

3. Open https://itunes.apple.com/lookup?id=807480077 where you replace the ID with the one you looked up.

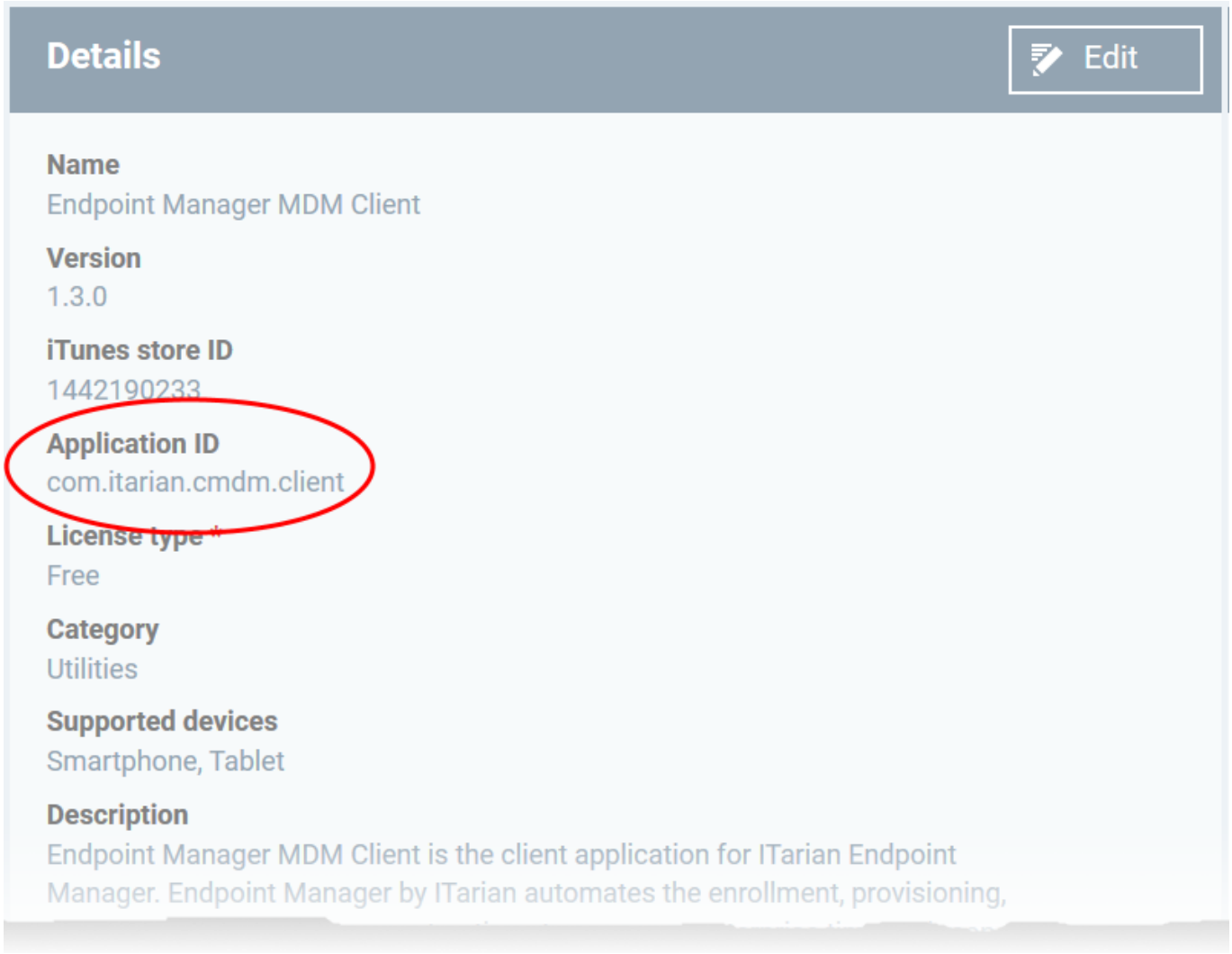
4. Search the output for "bundleID". In this example: "bundleId":"com.comodo.cmdm.client". So the Bundle ID is com.comodo.cmdm.client

Enterprise Application:

The App bundle ID can be viewed from the App Details screen of the App.

1. Click 'Application Store' from the left and choose 'iOS Store'

2. Click on the app from the list displayed at the right



The 'Application ID' field shows the bundle ID of the app.

Related topics:

How to specify allowed Wi-Fi networks for iOS devices