



ENDPOINT PROTECTOR

User Manual for Version 2.0.0.0

Mobile Device Management - User Manual



Table of Contents

1.Introduction.....	1
1.1. What is Endpoint Protector?	2
2.Activation of Mobile Device Management	3
2.1. Activation of Mobile Device Management Feature	4
3.How Endpoint Protector MDM Works	5
3.1. Supported Operating Systems and devices.....	6
4.MDM Setup APNS (Apple) & GCM (Google Android)	7
4.1. Setup of APNS for iOS and OS X	8
4.1.1. What is an Apple APNS Certificate and why do I need it?	8
4.1.2. How to generate your Apple APNS Certificate?	9
4.1.3. Renew an Apple APNS Certificate before expiration.....	11
4.2. Setup of GCM for Android.....	15
4.2.1. What is GCM (Google Cloud Messaging) and why I need it?.	15
4.2.2. How to get your Google API Key and Project Number for GCM and Maps?	16
4.2.3. Google C2DM	18
5.iOS EPP MDM App.....	19
5.1. EPP MDM iOS App Supported iOS Versions	19
5.2. EPP MDM iOS App to locate devices.....	19
5.3. EPP MDM iOS App to enroll devices (optional).....	20
5.4. EPP MDM iOS App Device Information.....	20
5.5. Installing the EPP MDM iOS App.....	21
5.6. Allow Location Services for EPP MDM iOS App.....	22
5.7. Pushing and Managing EPP MDM App to iOS Devices	22
6.Android Endpoint Protector MDM Client App	23
6.1. EPP MDM Android Client App Supported Versions	23
6.2. The Android EPP Client App	23
6.3. EPP Client Android App to enroll devices	23
6.4. Install EPP Client App on Android and Enrolling Android Device	24

7. Enrolling Mobile Devices	30
7.1. Different Enrollment methods are available:	31
7.2. Mobile Device Enrollment	32
7.2.1. iOS and OS X Enrollment and Profile Protection.....	34
7.2.2. iOS and OS X Profile Protection Deletion Passphrase	35
7.2.3. Sending E-Mail or SMS Enrollment Invitation (iOS/OS X / Android)	36
7.2.4. SMS Enrollment Number Format (iOS / Android)	37
7.2.5. E-Mail Enrollment Invitation (iOS/OS X / Android)	37
7.2.6. SMS Enrollment Invitation (iOS / Android)	38
7.2.7. iOS and OS X Mobile Device Enrollment over URL.....	39
7.2.8. iOS Mobile Device Enrollment through EPP MDM App	41
7.2.9. Android Device Enrollment.....	43
7.2.10. Bulk Enrollment	43
8. Managing Mobile Devices	47
8.1. Mobile Device Status	49
8.2. Mobile Devices Groups.....	53
9. Manage iOS Devices	54
9.1. Security Settings (Security Profile) on iOS.....	54
9.1.1. Password / Passcode Setting on iOS Device.....	55
9.1.2. Clear Passcode (No more password required)	55
9.1.3. iOS Device Hardware Encryption.....	55
9.2. Restrictions (Restrictions Profile) on iOS	56
9.2.1. The following iOS features can be restricted	57
9.2.2. The following Applications can be restricted.....	58
9.2.3. iCloud restrictions / Photo stream restrictions	58
9.2.4. Security and Privacy Restrictions	58
9.2.5. Content Rating Restrictions.....	58
9.2.6. iOS7 Restrictions	59
9.2.7. Supervised Device Restrictions	59
9.3. Remote iOS Lock of Device.....	60
9.4. Remote iOS Device Wipe (Device Nuke).....	60
9.5. iOS Disable Device Password / Passcode	61
9.6. Device Ownership	61

9.7. Voice Roaming on iOS	62
9.8. Profile Removal Policy for iOS Devices	62
9.9. Refresh App List for iOS	63
9.10. Installed Apps on iOS	64
9.11. Refresh Profile List on iOS	64
9.12. Profiles on iOS Devices Information	65
9.12.1. Mobile Devices > Profiles.....	65
9.12.2. Remove Profile from iOS Device	65
9.13. Manage Wi-Fi on iOS	65
9.13.1. Wipe Wi-fi Settings.....	66
9.14. Manage Mail on iOS.....	66
9.14.1. Wipe E-mail Settings	66
9.15. Manage VPN on iOS.....	67
9.16. Manage APN settings on iOS.....	67
9.17. Manage Cellular Settings on iOS devices	68
9.18. App Lock on iOS devices	69
9.19. History of iOS Devices Actions	69
9.20. Contacts and Accounts Tab on iOS Devices	70
10. Manage OSX Devices.....	71
10.1. Security Settings (Security Profile) on OS X	71
10.1.1. Password / Passcode Setting on OS X Device.....	72
10.1.2. OS X Device Hardware Encryption	72
10.2. File Vault 2 Disk Encryption on OS X.....	73
10.2.1. Disk Encryption Status.....	74
10.3. Remote Lock of Device	74
10.4. Remote OS X Device Wipe (Device Nuke).....	74
10.5. Device Ownership	75
10.6. Profile Removal Policy for OS X Devices	75
10.7. Refresh App List for OS X.....	76
10.8. Installed Apps on OS X	77
10.9. Refresh Profile List on OS X.....	77
10.10. Profiles on OS X Devices Information	77

10.10.1. Remove Profile from OS X Device.....	78
10.11. Manage Wi-Fi on OS X.....	78
10.11.1. Wipe Wi-fi Settings.....	78
10.12. Manage Mail on OS X.....	79
10.12.1. Wipe E-mail Settings	79
10.13. Manage VPN on OS X.....	79
10.14. History of OS X Devices Actions.....	80
11. Manage Android Devices.....	81
11.1. Security Settings (Security Profile) on Android.....	81
11.1.1. Password / Passcode Setting on Android Device	82
11.1.2. Device Password.....	83
11.1.3. Android Device Hardware Encryption.....	83
11.2. Request Storage Encryption	84
11.3. Remote Android Lock of Device.....	84
11.4. Device Ownership	86
11.5. Android Device Location Settings	86
11.5.1. Location Accuracy Fine on Android.....	86
11.5.2. Location Cost Allowed on Android	86
11.6. Manage Wi-fi.....	87
11.7. Manage Bluetooth Camera	87
11.8. Refresh Google Accounts for Android	87
11.9. Refresh App List for Android	88
11.10. Manage Calendar Events	88
11.11. Installed Apps on Android.....	89
11.11.1. Removing Installed Apps on Android.....	89
11.12. Get Contacts on Android.....	90
11.13. History of Android Device Actions	90
11.14. Manage Wi-Fi, Manage Mail, Profiles on Android	91
12. Mobile Application Management (MAM) for iOS	92
12.1. Adding Apps to your Managed Apps Catalog	93
12.1.1. Searching for Apps.....	93

12.1.2. Adding Apps to Managed Apps Catalog	94
12.1.3. Adding „Enterprise Apps“ to Managed Apps Catalog	94
12.2. Editing App Management Options	95
12.3. Managed Paid Apps	97
12.4. Pushing Apps to iOS Devices	99
12.4.1. Update Managed Apps / Changing Settings	100
12.5. Removing Managed Apps from iOS Devices	100
13. Android App Management	102
13.1 Adding Apps to your Managed Apps Catalog	102
13.1. Editing App Management Options	103
13.2. Pushing Apps to Android Devices	104
13.3. Removing Managed Apps from Android Devices	105
14. Policy Builder for iOS, OSX or Android Devices	106
14.1. Create a Policy for iOS, OS X or Android Devices	106
14.2. Assigning Devices to Policy	108
15. Unmanage a Mobile Device / Uninstall App 109	
15.1. iOS and OS X Device Unmanage by Administrator (over-the-air) 109	
15.1.1. iOS Uninstall / Unmanage by User (on Device)	109
15.1.2. OS X Uninstall / Unmanage by User (on Device)	110
15.2. Uninstall iOS EPP MDM app	110
15.3. Android EPP Client App Uninstall / Unmanage Android Device	110
16. Support	115
17. Important Notice / Disclaimer	116

1. Introduction

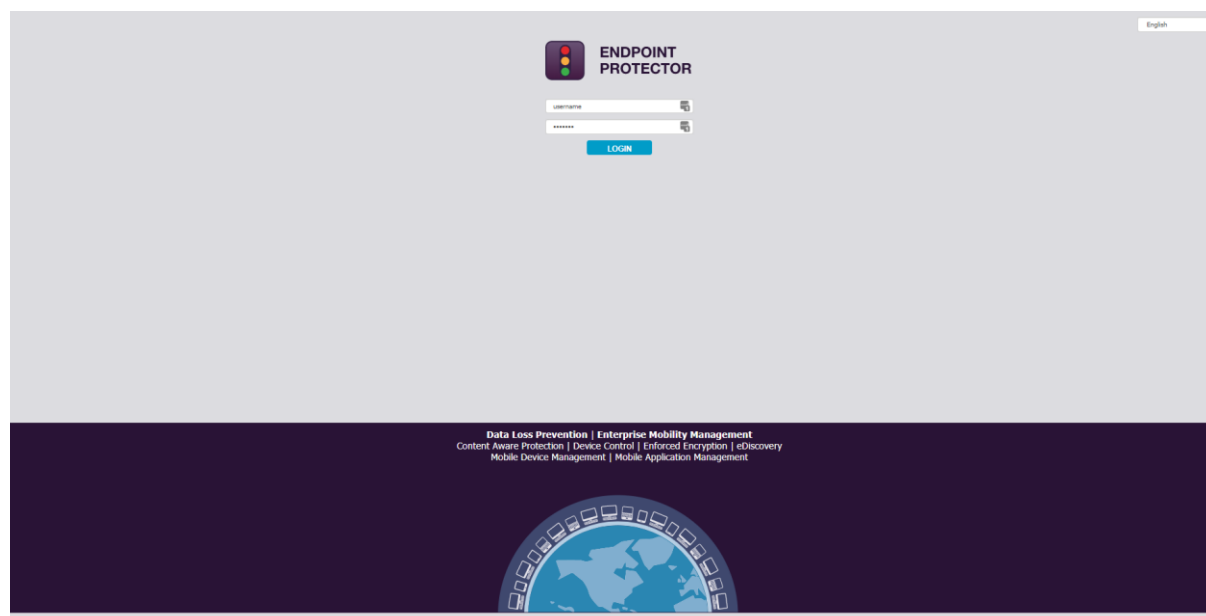
In the last past years, mobile devices have invaded business environments. Personally-owned or company owned smartphones and tablets are used on a daily basis by employees to store and have access to their company e-mails, sales reports etc. everywhere they go.

The wide adoption of the BYOD (Bring-Your-Own-Device) model by companies worldwide led to the use of more personal mobile devices by employees for storing business information together with private data such as photos and music. This trend raised new issues for IT administrators, which are faced now with the challenge of protecting sensitive company data not only inside the secured company network, but also everywhere it is taken on mobile company endpoints. At the same time, a separation and close monitoring of company information from personal data must be imposed.

To face the security challenges by the increase mobility in business environments, Mobile Device Management by Endpoint Protector enables a complete control and detailed monitoring over the use of mobile devices both inside and outside corporate environments, allowing employees to have a secure access to both corporate and private data wherever they are and on whatever device they are using without business critical information getting compromised.

1.1. What is Endpoint Protector?

Endpoint Protector is a complete Data Loss Prevention solution for companies' networks of all sizes, enabling a detailed control over removable, mobile storage media and mobile devices both inside and outside the companies' walls.

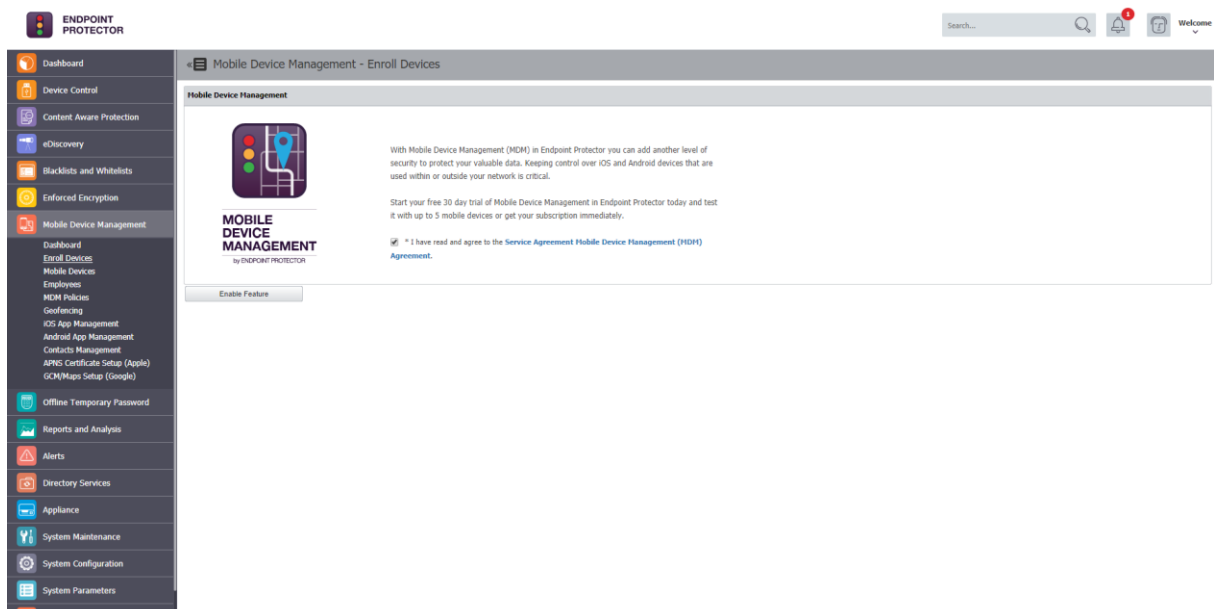


Endpoint Protector comprises three separate modules, which used together ensures the next generation security of your endpoints:

- **Mobile Device Management:** closely controls and monitors the entire mobile device fleet through dedicated MDM policies, protecting sensitive company data, while permitting a degree of freedom on what concerns the stored personal information. Once integrated in a company or enterprise network, it ensures a highly secure working environment for companies adopting and using the BYOD model.
- **Device Control:** enforces strong security policies for controlling and closely monitoring all portable storage device use inside the company network. Once deployed inside companies' networks, the Device Control modules reduces the risks of data loss and data theft through unauthorized use of removable and mobile devices through USB, etc.
- **Content Aware Protection:** allows defining custom content aware policies for a detailed inspection, detection and reporting of all sensitive content transfers outside the secured network. Once enabled, the Content Aware Protection module scans all possible exit points and ensures that no critical data leaves the company network either by transfers to removable media or directly via e-mail, file sharing applications or to the cloud.

2. Activation of Mobile Device Management

The Mobile Device Management feature enables administrators to remotely control and enforce strong security policies on iOS/OS X (Apple) and Android devices. Through options such as remote data wipe, device tracking and blocking, it offers enhanced protection against data theft and data loss, considerably reducing the risks that come with the increase of mobility in today's business environment.



The screenshot displays the Endpoint Protector web interface. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a search field, and user information. The left sidebar lists various management categories, with 'Mobile Device Management' selected. The main content area is titled 'Mobile Device Management - Enroll Devices' and features a 'MOBILE DEVICE MANAGEMENT by ENDPOINT PROTECTOR' logo. The text explains that MDM adds a security level for iOS and Android devices and offers a 30-day free trial. A checkbox for the 'Service Agreement Mobile Device Management (MDM) Agreement' is checked, and an 'Enable Feature' button is visible at the bottom.

2.1. Activation of Mobile Device Management Feature

Mobile Device Management comes as an optional feature with Endpoint Protector that requires a yearly-based separate subscription based on the number of protected mobile devices. By default, the feature appears as deactivated inside the Endpoint Protector Reporting and Administration interface.

The Mobile Device Management feature requires an internet connection for the Endpoint Protector Appliance.

The feature can be enabled by simply selecting the Mobile Device Management option from the left-side menu and clicking on the Enable Feature button.

Activating this feature will require a working Internet connection on Endpoint Protector Server/Appliance. Additionally, the initiator of the activation request will have to provide several company details such as Company Name, Contact Person Name and Contact Details, which will be sent to the Endpoint Protector Licensing Server including: Company name, Contact Person, Contact Details (phone number and e-mail). CoSoSys will use this information only for validation purposes and it will not imply subscribing to any newsletter or sharing it with any third party.

Once the request was processed and approved, the feature will be enabled by the CoSoSys Team. A notification will be sent to the provided e-mail address and the trial period for the feature will be activated.

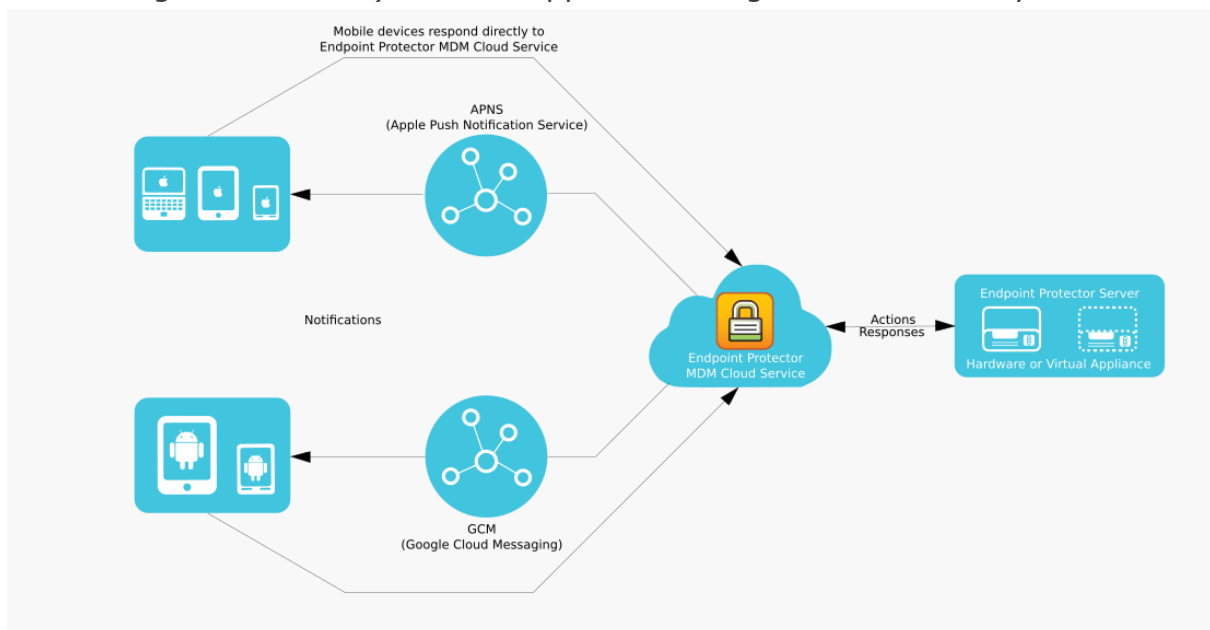
Please make sure your Firewall will have domains @cososys.com and @endpointprotector.com whitelisted for you to receive all communication.

A yearly subscription can be purchased to further use all the functionalities of the Mobile Device Management feature.

3. How Endpoint Protector MDM Works

For Endpoint Protector Mobile Device Management to be able to manage your mobile iOS, OS X and Android devices the communication between the devices and the Endpoint Protector Appliance over an internet connection is vital. Management actions need to arrive at your device either by a data connection like 3G in case of an iPhone or over an internet connection if the device does not have a data connection like an iPad (with Wi-Fi only), an Android tablet or a MacBook.

For the management actions to arrive at the device the actions are sent using for iOS and OS X devices the Apple Push Notification Service (short APNS) and for Android devices the Google Cloud Messaging Service (short GCM). To simplify the setup of your Endpoint Protector MDM service the Endpoint Protector Cloud is communicating between your Endpoint Protector Appliance (the Administration and Management Server) and the Apple and Google Services with your devices.



For the communication to work between your mobile devices and Endpoint Protector it is required that you setup the APNS and GCM settings as described in the following steps.

3.1. Supported Operating Systems and devices

The supported mobile device operating systems are:

- iOS5 + (iPhone and iPad)
- OS X 10.8 (Mountain Lion) and later macOS versions
- Android 4.4 + (Tablets and Phones)

4. MDM Setup APNS (Apple) & GCM (Google Android)

Before you can use the Endpoint Protector MDM features for iOS, OS X/macOS and Android different settings are required for you to make. The following chapter describes the steps and settings needed to be able to communicate between your mobile devices and the Endpoint Protector Mobile Device Management module.

⚠ Note

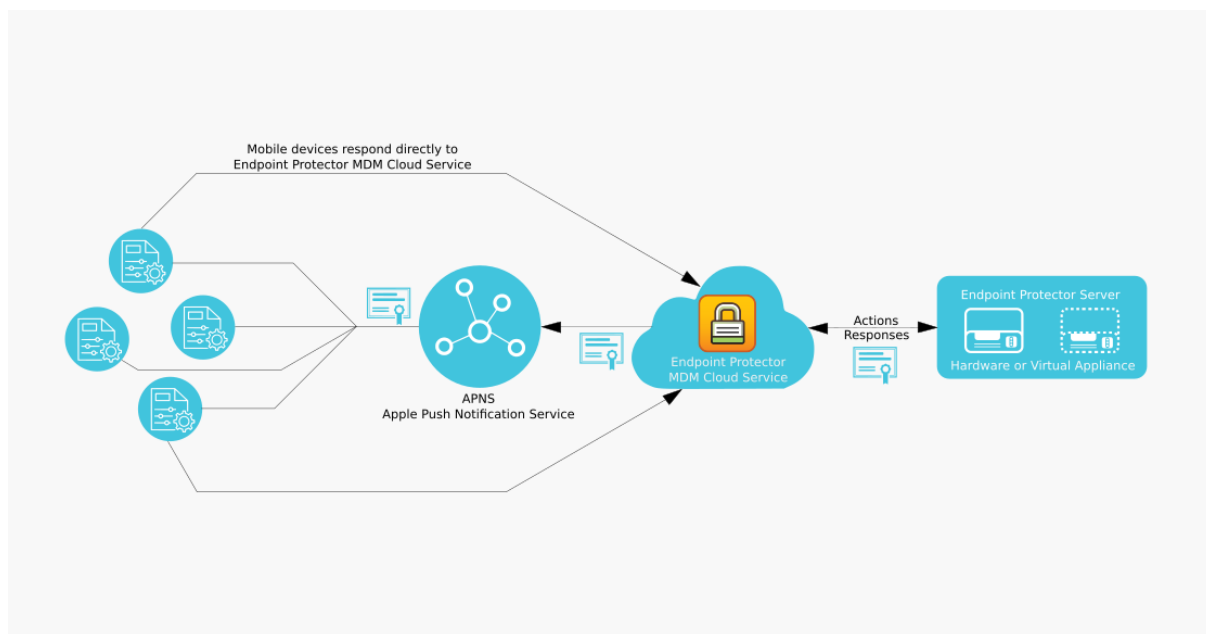
For Endpoint Protector Administrators that want to use the MDM Functionality only with Android devices the Apple APNS Setup (required for MDM with iOS or OS X) is **NOT REQUIRED**. If you want to use Endpoint Protector MDM with iOS/ OS X and Android devices the setup of both GCM (Google Cloud Messaging for Android) and Apple APNS is required.

4.1. Setup of APNS for iOS and OS X

4.1.1. What is an Apple APNS Certificate and why do I need it?

In order to use the MDM features provided for iOS or OS X an Apple Push Notification Service (short APNS) certificate is required by Apple Inc. Receipt of the Apple issued and signed certificate is up to Apple Inc. own discretion.

What is Apple APNS? It is a certificate that is signed by Apple to clearly identify what iOS or OS X devices are communicating with your Endpoint Protector Appliance in order to be sure that only your company own devices receive commands from Endpoint Protector MDM.



4.1.2. How to generate your Apple APNS Certificate?

The APNS Certificate can be generated in just a few simple steps from the Mobile Device Management – APNS Certificate Setup (Apple).

The screenshot shows the Endpoint Protector Administration Interface. The left sidebar contains various management options, with 'APNS Certificate Setup (Apple)' highlighted in red. The main content area is titled 'Mobile Device Management - APNS Certificate Enrollment' and contains the following steps:

- Step 1 - Fill in this form below with your company information for a CSR**: This step requires filling out a form with company details. The form fields are: Company Name (California), E-mail (your.email@company.com), Country (United States), State or Province Name (New York), and Location (City) (New York City). A 'Download signed CSR' button is located below the form.
- Step 2 - Request your signed certificate for APNS from Apple**: This step involves signing the certificate for your company to be used with Apple Push Notification Services (APNS) and linking the certificate to your Apple ID. It provides a URL for the Apple website and instructions on how to obtain the certificate.
- Step 3 - Upload certificate signed by Apple**: This step requires uploading the signed certificate received from Apple. It includes a 'Choose File' button and an 'Upload' button.

Note

We recommend performing these steps on a Safari or Mozilla Firefox browser. Use of Internet Explorer for this step is known to cause the process to fail.

1. In the Administration Interface, go to Mobile Device Management and select APNS Certificate Setup (Apple), where you have to complete the enrollment for the Apple Push Notification Certificate.
2. Fill in the required details and click on the "Download signed CSR" to get the Code Signing Request (CSR) file signed by CoSoSys. Save it on your computer.

Step 1 - Fill in this form below with your company information for a CSR

CoSoSys as authorized MDM vendor will sign for you a Certificate Signing Request (CSR) in this step. You will need this in the next step when contacting Apple.

All fields are mandatory.

Company Name:	Your Company
E-mail:	your.email@yourcompany.com
Country:	United States
State or Province Name:	New York
Location (City):	New York City

Download signed CSR

3. In a different browser window open the following link to the Apple Push Certificates Portal: <https://identity.apple.com/pushcert/>

Step 2 - Request your signed certificate from Apple for APNS

Apple will sign the certificate for your company to be used with Apple Push Notification Services (APNS) and will link the certificate to your Apple ID.

Visit this dedicated Apple website for this here: <https://identity.apple.com/pushcert> log in with your Apple ID and follow the steps to obtain your certificate for APNS. In this step provide Apple with the certificate you have downloaded in step 1 above.

4. Login to the Apple Push Certificates Portal using your Apple ID and follow the steps provided there.
5. Click "Create a Certificate" and agree to the Apple Terms of Use.
6. Select your signed CSR (downloaded at step 2) and click "Upload to the Apple Push Certificates Portal" that you saved on your computer. In just a few moments, your certificate will be available for download.
7. Download now the Certificate from the Apple Push Certificates Portal to your computer.
8. The APNS certificate from the previous step has to be uploaded to the Endpoint Protector MDM Setup.

Step 3 - Upload certificate signed by Apple

Upload now the certificate you received signed from Apple in step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.

Browse for APNS certificate signed by Apple:

After the upload was successfully performed, your setup for the Endpoint Protector Mobile Device Management is finalized for iOS and OS X.

You can now start enrolling iOS and OS X devices by sending invitations to them either by E-Mail or SMS or through the other supported enrollment methods as described in the following paragraph 7. Enrolling Mobile Devices.

4.1.3. Renew an Apple APNS Certificate before expiration

The Apple APNS certificate must be renewed periodically with Apple before its expiration date to avoid losing control over the managed iOS and OS X devices or having to re-enroll all devices.

Please check the expiration date of your APNS certificate in the Endpoint Protector interface.

The screenshot displays the Endpoint Protector interface for Mobile Device Management - APNS Certificate Enrollment. A green notification bar at the top states: "Request was successful. Your APNS Certificate will expire on 2020-10-17 16:12:15. Be sure to renew it before this date." The main content area is divided into three steps:

- Renew:** A warning that the APNS certificate must be renewed with Apple before its expiration date. It notes that if the certificate expires or is revoked, the user will lose control over managed iOS and OS X devices. It advises completing steps with "Safety or Privilege to avoid errors".
- Step 1 - Fill in this form below with your company information for a CSR:** A form for creating a Certificate Signing Request (CSR). It includes fields for Company Name, E-mail, Country, State or Province Name, and Location (City). A "Download signed CSR" button is at the bottom.
- Step 2 - Request your signed certificate for APNS from Apple:** Instructions to visit the Apple website (<https://identity.apple.com/pushcert>) to request a signed certificate for APNS.
- Step 3 - Upload certificate signed by Apple:** Instructions to upload the signed certificate received from Apple. It includes a "Choose File" button and an "Upload" button.

The APNS certificate can be renewed in just a few simple steps from the Mobile Device Management – APNS Certificate Setup (Apple) in Endpoint Protector.

Note

If your APNS certificate expires or is revoked, it will result in unmanaged iOS and OS X devices. To manage a device after an APNS certificate expires requires re-enroll of the iOS or OS X device.

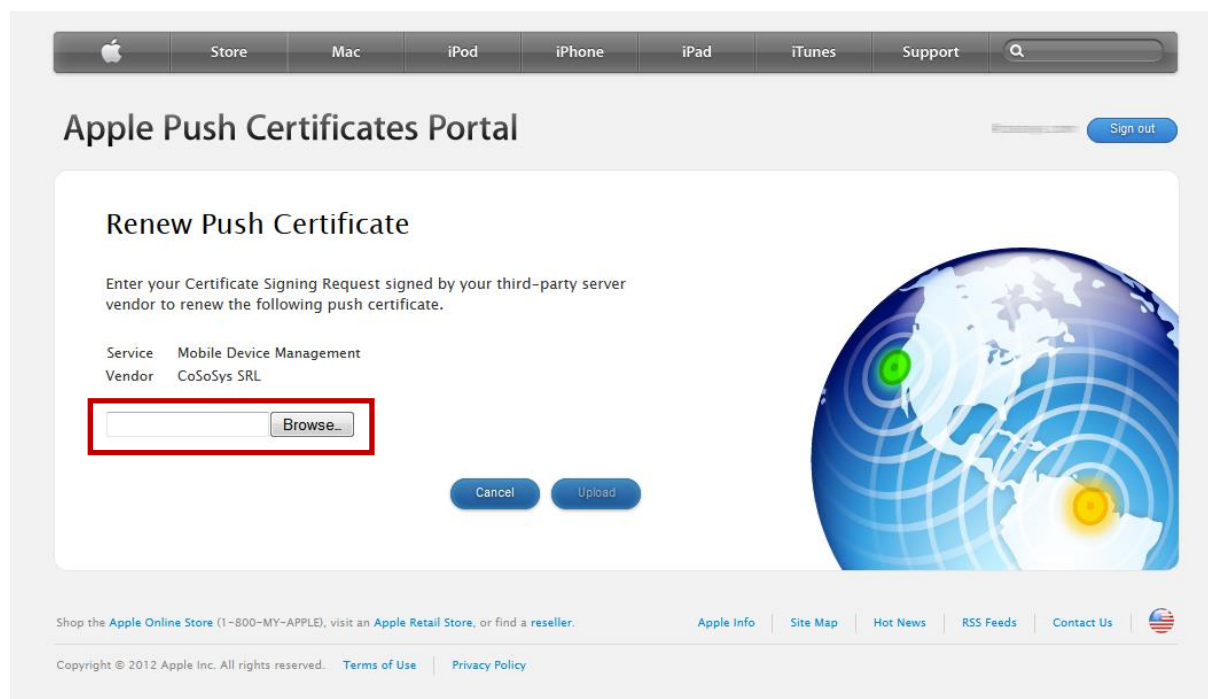
Note

We recommend performing these steps on a Safari or Mozilla Firefox browser. Use of Internet Explorer for this step is known to cause the process to fail.

1. In the Endpoint Protector Administration Interface, go to Mobile Device Management and select APNS Certificate Setup (Apple) setup.
2. Renew your APNS Certificate before it expires by checking the expiration date as mentioned in the interface.
3. Follow the same steps as you have in the initial enrollment process. Click on the "Download signed CSR" to get the Code Signing Request (CSR) file signed by CoSoSys. Save it on your computer.
4. In a different browser window (Firefox or Safari browser, not Internet Explorer!) open the following link to the Apple Push Certificates Portal: <https://identity.apple.com/pushcert/>
5. Login to the Apple Push Certificates Portal using your Apple ID (previously used to request an APNS Certificate) and follow the steps provided there.
6. Click "Renew".

The screenshot shows the Apple Push Certificates Portal interface. At the top, there is a navigation bar with links for Store, Mac, iPod, iPhone, iPad, iTunes, and Support, along with a search icon. Below this is the main header "Apple Push Certificates Portal" and a "Sign out" button. The main content area is titled "Certificates for Third-Party Servers" and features a "Create a Certificate" button. A table lists certificates with columns for Service, Vendor, Expiration Date*, Status, and Actions. The first row shows a certificate for "Mobile Device Management" from "CoSoSys SRL" with an expiration date of "Feb 21, 2013" and a status of "Active". The "Actions" column for this certificate contains three buttons: "Renew", "Download", and "Revoke". The "Renew" button is highlighted with a red rectangular box. Below the table, a note states: "*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate." Below this is a section titled "About Apple Push Certificates Portal" with two paragraphs of text and links. The first paragraph says "Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices." and includes a link "Learn more about Mobile Device Management". The second paragraph says "MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal." and includes a link "Learn more about MDM push certificate migration". To the right of this text is a graphic of a globe with a green location pin and a yellow sun. At the bottom of the page, there is a footer with links for "Shop the Apple Online Store", "Apple Info", "Site Map", "Hot News", "RSS Feeds", "Contact Us", and "Terms of Use", along with a copyright notice for 2012 Apple Inc.

7. After clicking "Renew" you are prompted to upload the Code Signing Request (CSR) from the previous step 3 that you saved on your computer. Select your signed CSR and click "Upload to the Apple Push Certificates Portal". In just a few moments, your certificate will be renewed and you see the Expiration date is updated.



8. Download now the Certificate from the Apple Push Certificates Portal to your computer.

Apple Push Certificates Portal

Sign out

Certificates for Third-Party Servers

Create a Certificate

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	CoSoSys SRL	Feb 21, 2013	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
[Learn more about Mobile Device Management](#)

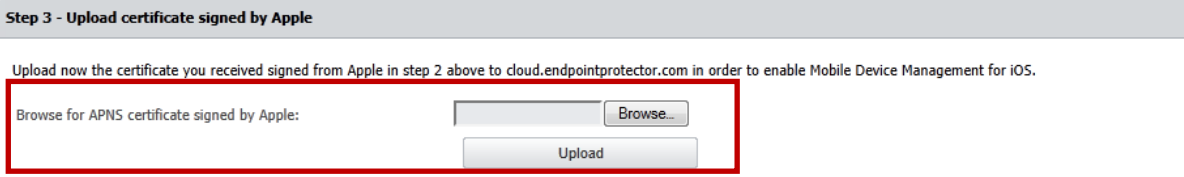
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
[Learn more about MDM push certificate migration](#)

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a reseller.

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#)

Copyright © 2012 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

9. The APNS certificate from the previous step has to be uploaded to the Endpoint Protector/My Endpoint Protector MDM Setup.



Step 3 - Upload certificate signed by Apple

Upload now the certificate you received signed from Apple in step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.

Browse for APNS certificate signed by Apple:

After the upload was successfully performed, your APNS renewal for the Mobile Device Management is finalized.

Please check if the expiration date of the APNS certificate in Endpoint Protector/My Endpoint Protector was updated to the renewed date.

4.2. Setup of GCM for Android

To use Mobile Device Management features for Android devices it is required that you provide an API key from Google. This API key is also required if you want to see device locations (using Google Maps) for Android and iOS devices in the "Locate Mobile Device View" of Endpoint Protector.

4.2.1. What is GCM (Google Cloud Messaging) and why I need it?

In order to use the MDM features provided for Android a GCM API Key (Google Cloud Messaging for Android) is required. GCM is necessary to establish communication between an Android mobile device and Endpoint Protector and issuance to you is up to Google/Androids own discretion.

For more info about Google Cloud Messaging for Android, please refer to: <http://developer.android.com/guide/google/gcm/index.html>

For more info about Google Maps API, please refer to: <https://developers.google.com/maps/>

4.2.2. How to get your Google API Key and Project Number for GCM and Maps?

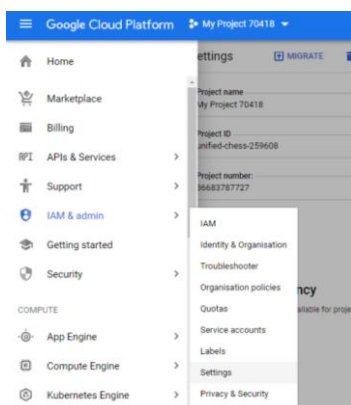
Step 1 - Create and enable Google Cloud Platform Project

<https://cloud.google.com/apis/docs/getting-started>

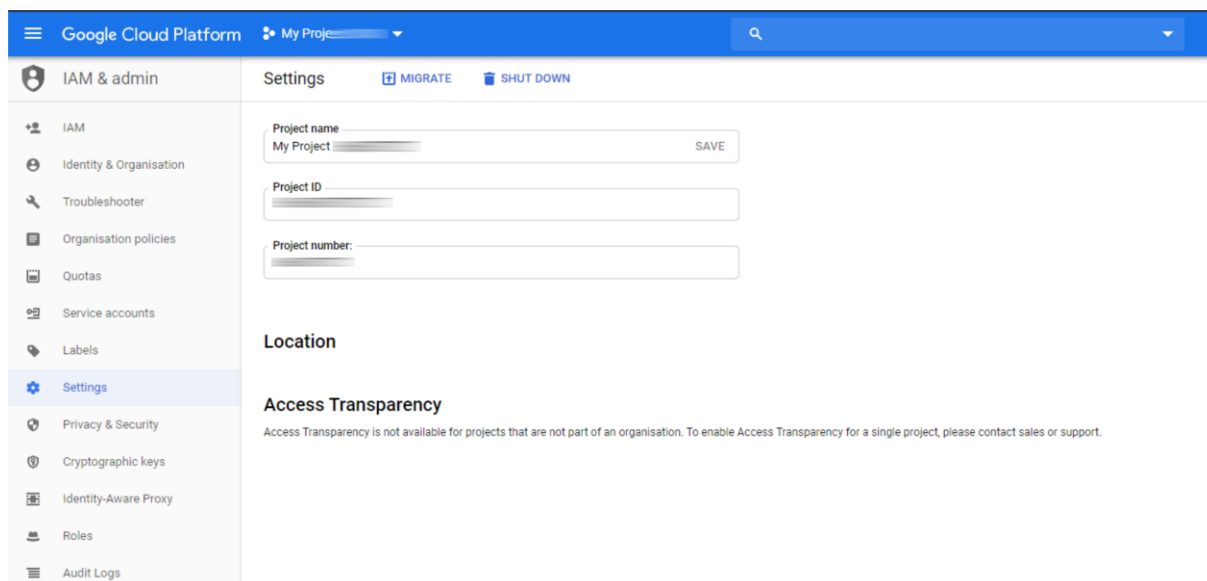
Step 2 - Go to <https://cloud.google.com>

The menu is always changing, but it should be visible to see and create a new project. Give it a name and it will be automatically attached a Project Number.

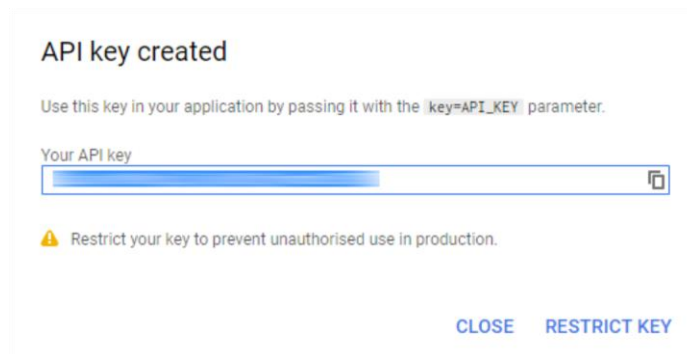
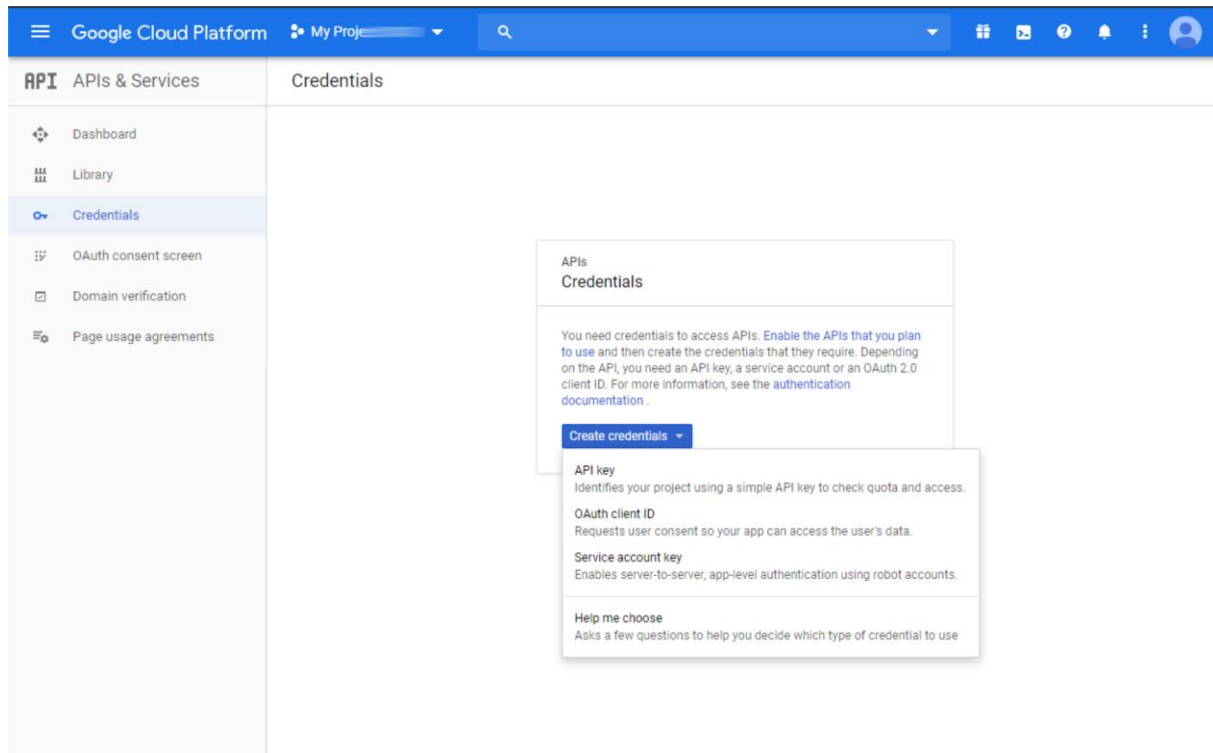
Step 3 - Once the project is created, make sure that is also selected. You can check that, it should be visible the name of the Project, right by the Google Cloud Platform logo, left side of the page.



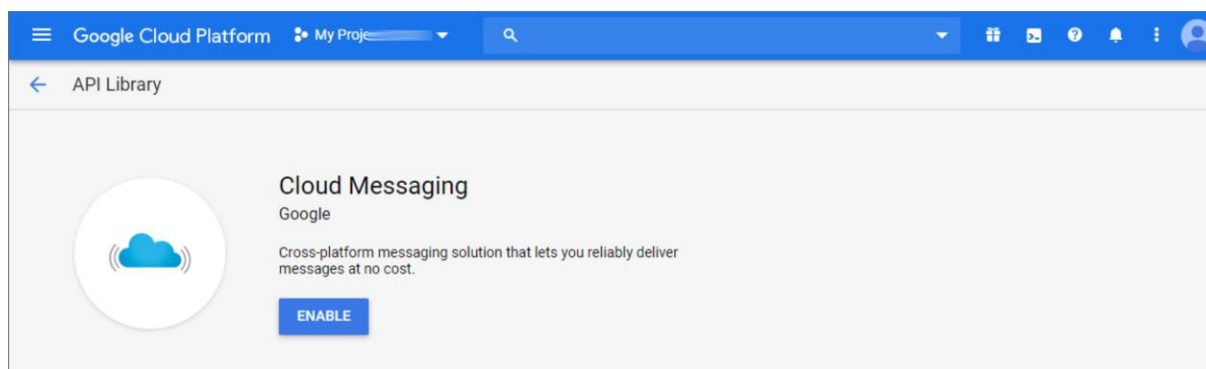
Step 4 - If you click the navigation menu (hamburger menu, top left), you'll see the complete list of options for your account. Go to IAM & Admin and select the Settings menu item. Here you'll find the Project Number. Copy that and put it in our EPP server, on the GCM page.



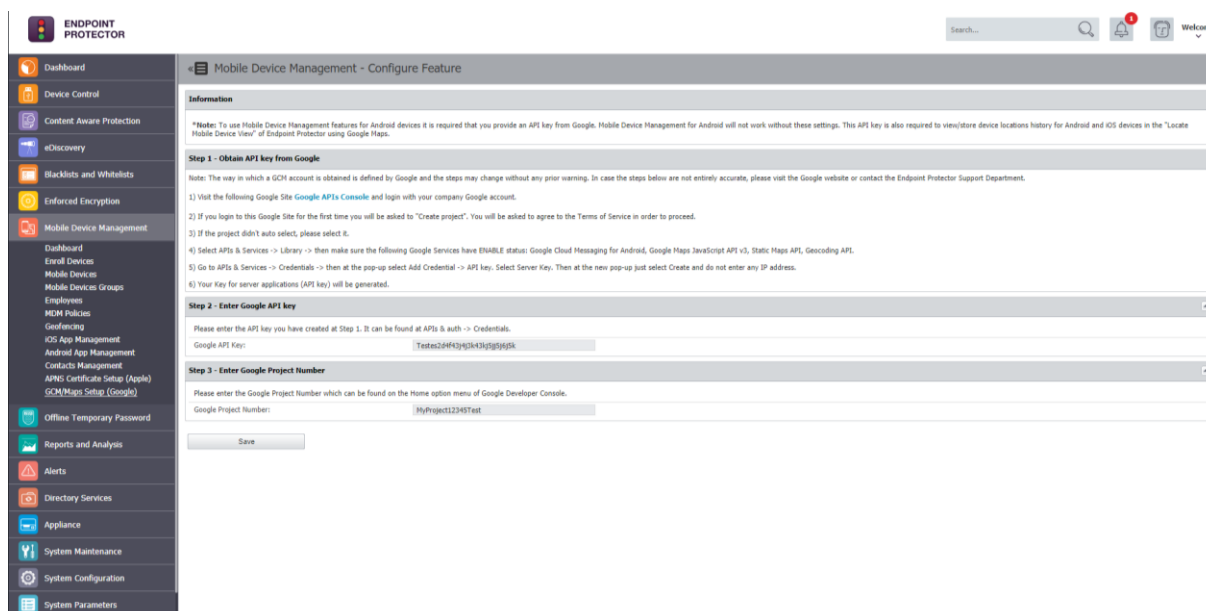
Step 5 - Next if you click the navigation menu, you see the APIs and Services, from here click on the Create Credentials and select API key. This page will create an API key for us to put in the EPP server, on the GCM pages and authenticate the communication between Google Cloud Platform and the EPP server.



Step 6 - Now if you click on the navigation menu, go again to the APIs and Services, the go to the Library item and search for the services: Google Cloud Messaging for Android, Google Maps JavaScript API v3, Static Maps API, Geocoding API and enable them. This APIs are need for messaging, for Maps and for calculating the addresses.



Step 6 – Once you have the API key and Project Number, the GCM/Maps Setup configuration can be fulfilled on the Endpoint Protector server side.



4.2.3. Google C2DM

C2DM for Android is not supported by Endpoint Protector anymore.

5. iOS EPP MDM App

The EPP MDM iOS app is a free app for iOS available on the Apple App Store. The EPP MDM app is compatible with iPhone and iPad. It is an optional app and not a necessity for use of Endpoint Protector MDM for iOS. The EPP MDM app has two functions, one to locate the device and second to use the app optionally also as a way to enroll an iOS device to Endpoint Protector Mobile Device Management.

5.1. EPP MDM iOS App Supported iOS Versions

The EPP MDM app for iOS supports iOS version 7.0, 6.0, 5.0. iOS version 4.0 is not supported by the EPP MDM iOS app due to missing support for required features.

5.2. EPP MDM iOS App to locate devices

The EPP MDM app allows the iOS device to provide location data of the device to the Endpoint Protector Appliance in order to determine the current location of an iOS device in case it is misplaced, lost or stolen. To locate an iOS device the EPP MDM app is a necessity on the iOS device.



5.3. EPP MDM iOS App to enroll devices (optional)

The EPP MDM App allows the iOS device to enroll as described below at “iOS Mobile Device Enrollment through EPP MDM App”. The EPP MDM App is not required for enrollment, it is simply an option to enroll in this way a device to Endpoint Protector Server.

5.4. EPP MDM iOS App Device Information

The EPP MDM app also detects device details and if a device was tampered with (Jailbreak Status).



5.5. Installing the EPP MDM iOS App

The EPP MDM app for iOS is available on the Apple App Store here:

<https://itunes.apple.com/us/app/epp-mdm/id570954584?mt=8>

Downloading and installing the application can be made directly on the iOS device by accessing App Store on the device, and entering EPP MDM in the search bar. The search result will show you EPP MDM by CoSoSys.

Click on the button "FREE" followed by "INSTALL APP". After that the EPP MDM app will be downloaded and installed on your device.

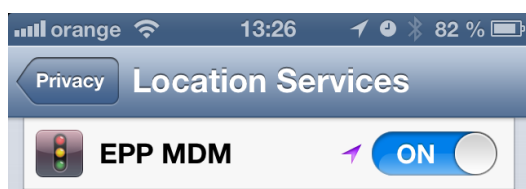
To start the EPP MDM app simply locate it on your iOS device home screen and click to start it.



5.6. Allow Location Services for EPP MDM iOS App

After starting the EPP MDM iOS app the user will be asked “EPP MDM would like to use your current location”. The user has to select “OK” to allow Location Services. If this setting is not made correctly to allow the iOS EPP MDM app will not be able to report location information.

This setting can be checked on the iOS device in the following location: iOS device home screen > Settings > Privacy > Location Services. Location Services have to be set to “ON” and for the EPP MDM set to “ON” as well. Next to the “ON” a small compass needle icon is shown as well.



5.7. Pushing and Managing EPP MDM App to iOS Devices

The EPP MDM App can be pushed and managed to any supported and managed iOS device.

For details how to push the EPP MDM App to an iOS device check section 12.4 (Pushing Apps to iOS Devices).

6. Android Endpoint Protector MDM Client App

The Android **Endpoint Protector MDM Client** app is a free app for Android and available on the Google Play Marketplace here:

<https://play.google.com/store/apps/details?id=com.cososys.eppclient&hl=en>

The Android EPP Client app is MANDATORY for use of Endpoint Protector MDM with Android devices.

6.1. EPP MDM Android Client App Supported Versions

The EPP MDM app for Android is compatible with Android devices using Android Version 2.2 (Codename Froyo) or newer.

6.2. The Android EPP Client App

The Android EPP Client app allows the Android device to provide Endpoint Protector MDM with management rights. It also offers location data of the device to the Endpoint Protector Appliance in order to determine the current location of an Android device in case it is misplaced, lost or stolen.

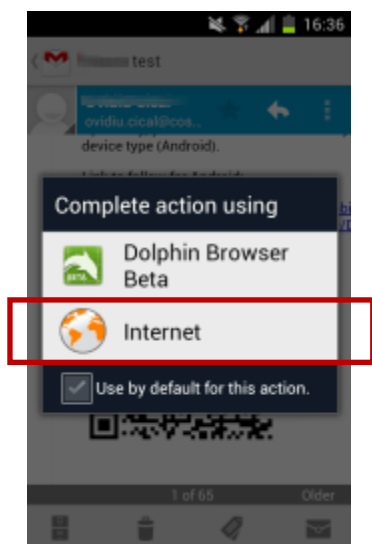
6.3. EPP Client Android App to enroll devices

The Android EPP Client App is required for enrollment of an Android mobile device to an Endpoint Protector Appliance.

6.4. Install EPP Client App on Android and Enrolling Android Device

After receiving the enrollment invitation E-Mail or SMS click on the link provided in the E-Mail or SMS.

1. Choose to open the link with the default browser on your Android device.



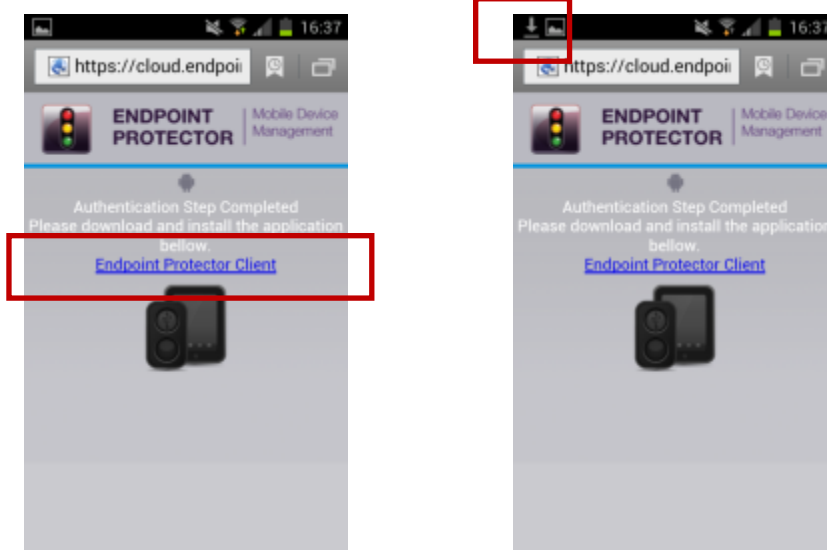
In this case (screenshot above) the choice for native browser is the option “Internet”, not the Dolphin or any other browser that might be installed on your Android device.

2. The web browser will open the enrollment site that already includes your registration data consisting of an MDM ID and your One Time Code (OTC).

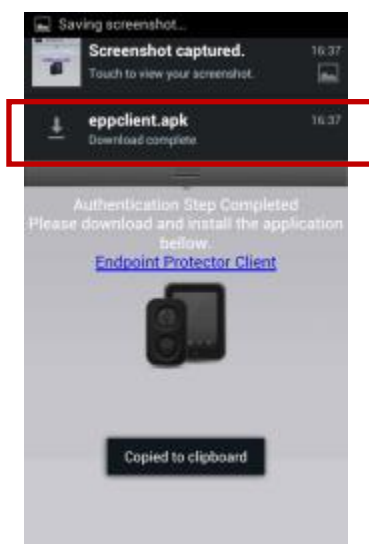


Click “Connect” to proceed”

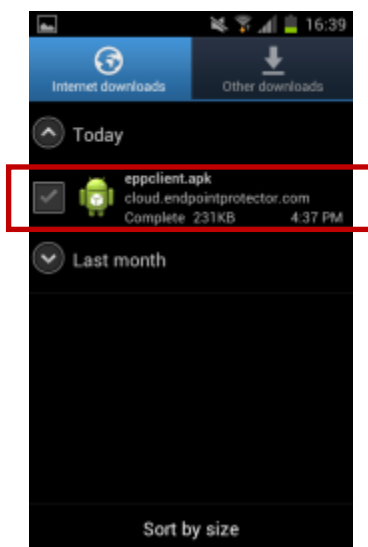
3. In the next step the device user has to click on the “Endpoint Protector Client” link. Then a download of the EPP Client App will start.



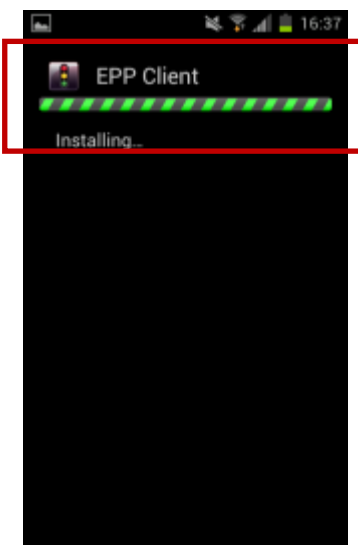
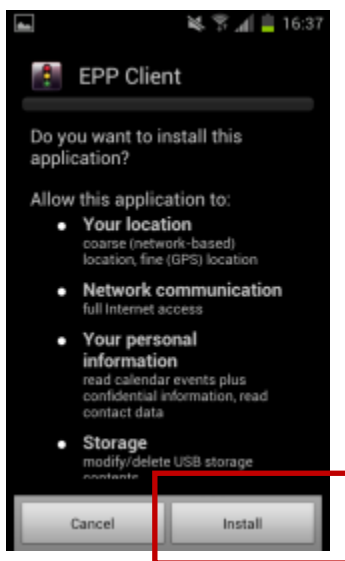
4. The download of the `epclient.apk` (name of the EPP Client Android app download file) should finish rather fast depending on your data connection speed since the `epclient.apk` is small.



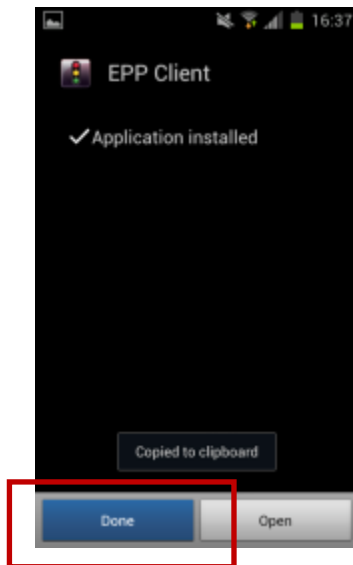
5. Locate now the eppclient.apk in the download folder on your device.



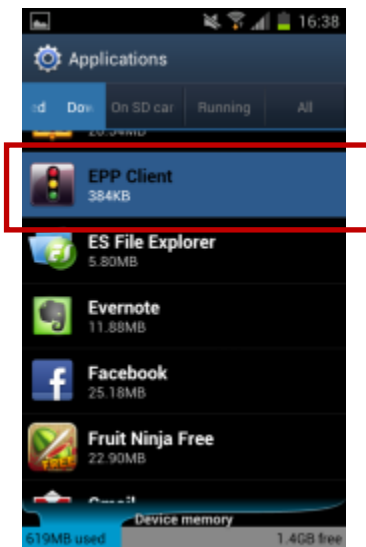
6. Click on the eppclient.apk and select "Install". The EPP Client will start to install itself on the Android device.



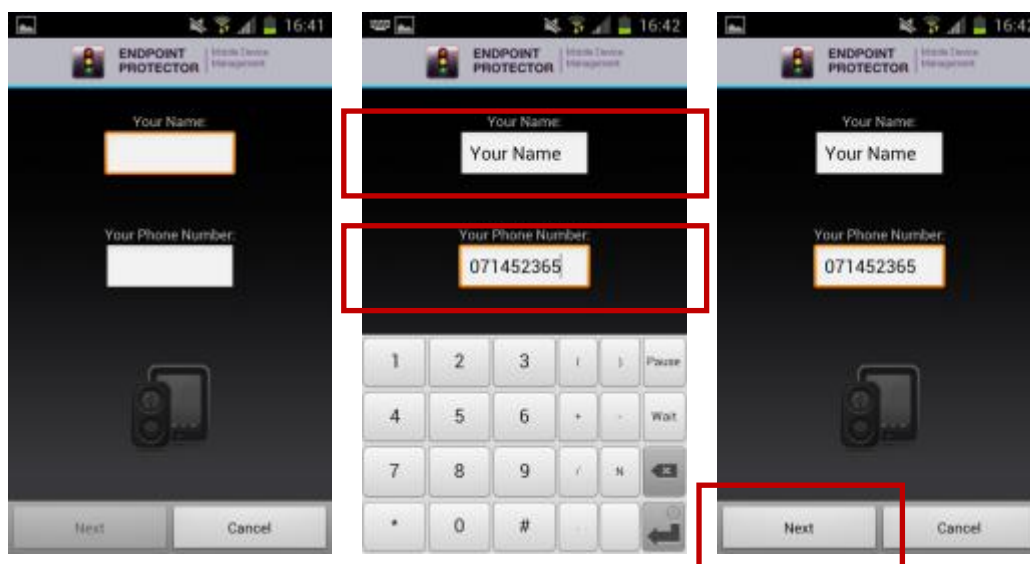
7. After the installation you will see a message indicating the installation is finished. Click “Done” to complete the final steps for your Android device enrollment.



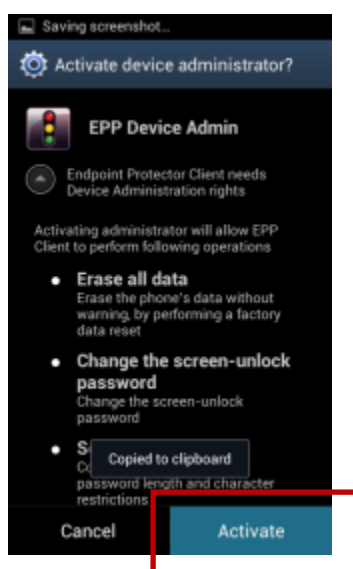
8. Go to “Applications” on your Android device. There locate the EPP Client and start it.



9. After the EPP Client starts you need to fill in your Name and your Phone Number. If the device has no phone number provide your mobile number for the Administrator to easier link your device with you as a user. Click "Next" after you completed the fields.



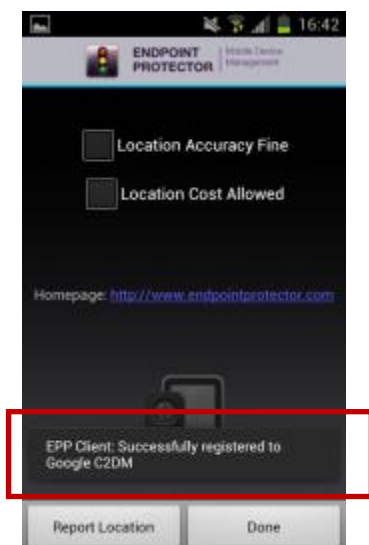
10. Now the question regarding device administration will appear which needs to be confirmed by clicking "Activate".



Note

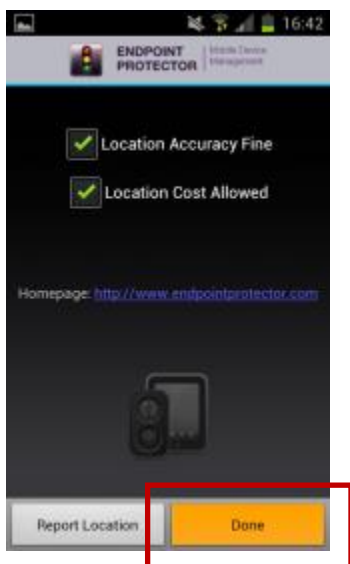
By not enabling this option, the Android mobile device cannot be remotely administrated / managed.

11. Now you will see the message “EPP Client Successfully registered to Google GCM or C2DM”. This means that your Android device is now enrolled.



12. The settings “Location Accuracy Fine” or “Location Cost Allowed” can be selected.

Click “Done” to finish the enrollment process.

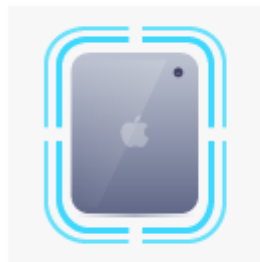


These two settings are described in the chapter 11.5.1 Location Accuracy Fine on Android 11.5.2 Location Cost Allowed on Android.

7. Enrolling Mobile Devices

Enrolling Mobile Devices means to establish the connection for communication and management between the Endpoint Protector Appliance and your mobile devices. It is the process of inviting, enrolling and connecting the device with your Endpoint Protector Appliance.

IOS enrollment



Android enrollment



To enroll mobile devices it is required to have the setup for either APNS (for iOS and OS X) or GCM (for Android) as described in chapter 4. MDM Setup APNS (Apple) & GCM finalized. If the Setup for APNS or GCM is not finalized the Endpoint Protector Appliance will not give you access to > Enroll Devices.

7.1. Different Enrollment methods are available:

A mobile device can be enrolled by:

1. Accessing a link in the invitation E-mail send to the device
2. Scanning a QR code contained in the invitation E-mail for a device
3. Accessing a link contained in the invitation SMS send to the device
4. Accessing directly a link through the native web-browser on the device and completing the Endpoint Protector ID and OTC fields
 - a. For iOS devices the link is:
<https://cloud.endpointprotector.com/mobile.php/register/iOS>
 - b. For OS X devices the link is:
<https://cloud.endpointprotector.com/mobile.php/register/OSX>
 - c. For Android devices the link is:
<https://cloud.endpointprotector.com/mobile.php/register/android>
5. Downloading and installing the EPP MDM app on an iOS, OS X or Android device and completing the Endpoint Protector ID and OTC fields

Note

Enrollment of iOS and OS X devices should be done through the Safari browser on your iOS and OS X device. Other browsers are not supported. For Android devices enrollment should be done through the native web browser on the device.

7.2. Mobile Device Enrollment

To be able to manage mobile phones and tablets, each device must be enrolled by going to Mobile Device Management -> Enroll Devices option.

The screenshot displays the 'Mobile Device Management - Enroll Devices' page. The 'Mobile Device Management Information' section shows the MDM ID (highlighted with a red box) and device counts for iOS/iOS, Android, and Mac. The 'Enroll Mobile Devices' section provides instructions for enrolling devices via email, SMS, or QR code, with a QR code image and radio buttons for device type selection. The 'One Time Codes' section contains a table of enrollment codes.

Code	Uninstall Password (Show)	Requested at	Actions
88805	*****	18 October 2019 11:07	<input type="checkbox"/>
E1069	*****	18 October 2019 11:07	<input type="checkbox"/>
58809	*****	18 October 2019 11:07	<input type="checkbox"/>
F2803	*****	18 October 2019 11:07	<input type="checkbox"/>
88809	*****	18 October 2019 11:07	<input type="checkbox"/>
F2AMA	*****	18 October 2019 11:07	<input type="checkbox"/>
5WQ12	*****	18 October 2019 11:07	<input type="checkbox"/>
EUR5U	*****	18 October 2019 11:07	<input type="checkbox"/>
88774	*****	18 October 2019 11:07	<input type="checkbox"/>
ELWMP	*****	18 October 2019 11:07	<input type="checkbox"/>

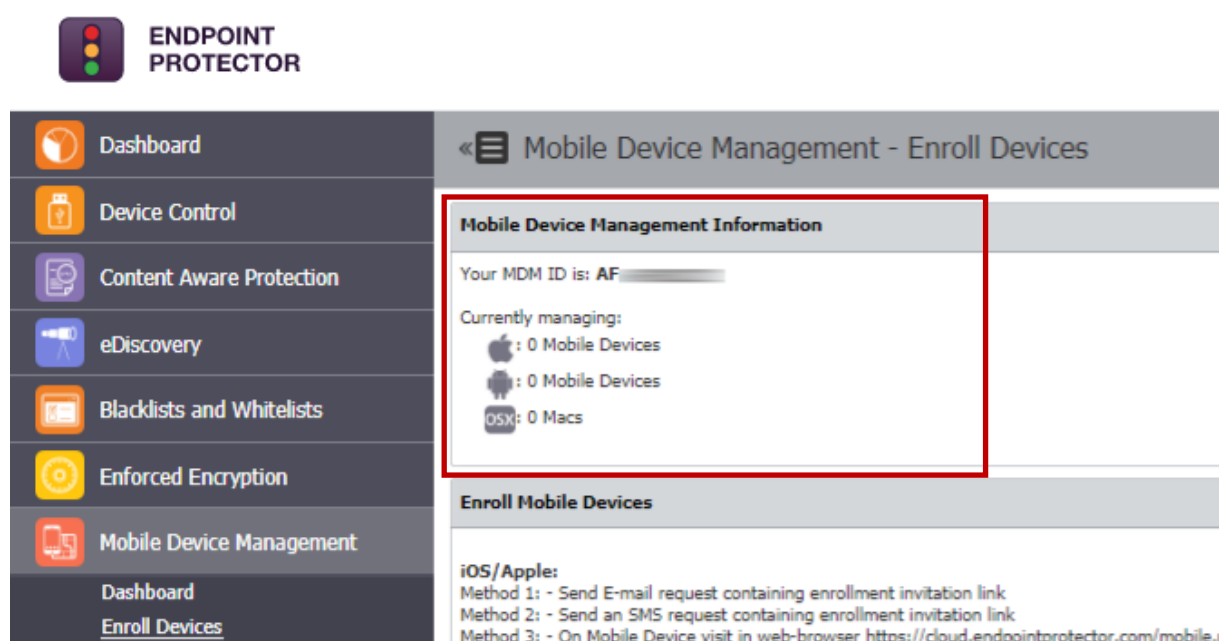
In the Enrollment window, under Mobile Device Management Information, the MDM ID corresponding to your appliance is displayed, which will be further used as a parameter for enrolling mobile devices. Additionally, one can check the exact number of mobile devices enrolled at that moment.

The enrollment of iOS, OS X and Android devices is similar in many ways. There are different enrollment options for each mobile device type available. The first two options allow the sending of E-mail and SMS based invitation requests to mobile devices, invitations which include short instructions on the steps required for the end users of the device to perform. The sending of E-mail invitations can be performed by clicking on the "Send E-mail request" button, while the SMS based invitation can be performed by clicking on the "Send SMS Request" button. The "Bulk Enrollment" feature allows the administrator to send mass enrollment requests with just a few clicks. The administrator must create a contact list, either by pasting it into the contacts list field, or by importing it. After the contacts are added, either way, they will be shown in the interface, and with the "Add to sending queue" button the "Bulk Enrollment" process can be started and the invitations will be sent to all contacts (more on "Bulk Enrollment" at paragraph 7.2.10).

In order to ensure that a mobile device is properly and securely enrolled, there are two keys required during the enrollment process:

- **MDM ID** – which uniquely identifies your Endpoint Protector Appliance/Server.
- **OTC (One-Time-Code)** – which allows only the invited devices to be enrolled on your Endpoint Protector Appliance/Server. The OTC will expire after one use.
- **Uninstallation Passphrase (applies to iOS and OS X)** – which allows the device to be unmanaged / uninstalled. The uninstallation option for iOS and OS X has to be chosen at enrollment time.

The MDM ID can be found in the Reporting and Administration web interface at: Mobile Device Management > Enroll Devices > Mobile Device Management Information



The screenshot shows the Endpoint Protector web interface. The left sidebar contains navigation options: Dashboard, Device Control, Content Aware Protection, eDiscovery, Blacklists and Whitelists, Enforced Encryption, and Mobile Device Management. The main content area is titled "Mobile Device Management - Enroll Devices". A red box highlights the "Mobile Device Management Information" section, which displays:

- Your MDM ID is: AF-
- Currently managing:
 - iOS: 0 Mobile Devices
 - Android: 0 Mobile Devices
 - OSX: 0 Macs

Below this information is the "Enroll Mobile Devices" section, which lists three methods for iOS/Apple:

- Method 1: - Send E-mail request containing enrollment invitation link
- Method 2: - Send an SMS request containing enrollment invitation link
- Method 3: - On Mobile Device visit in web-browser <https://cloud.endpointprotector.com/mobile>

These invitations, in case of an unknown device type and E-mail request, will include three different registration links for the different types of devices (iOS, OS X and Android), which readily include the MDM ID and OTC. In case of an unknown device type and SMS request, the invitations will include two different registration links for iOS and Android, which already holds the MDM ID and OTC.

While the MDM ID is used for all enrolled mobile devices, different OTCs must be used for enrolling each mobile device. The Mobile Device Management feature comes with 10 pre-generated OTCs available in the Enrollment window. The "Request More OTC" option will allow the Administrator to generate more OTCs.

Once an E-mail or SMS based invitation request is sent, an OTC will be automatically assigned to the user requesting the enrollment of his device and it

will be automatically removed from the list of available One Time Codes. To verify which OTC was assigned to each device and user, the administrator can click on the “View Sent Invitations” button, which will display a list of all used OTCs with the corresponding e-mail addresses and/or phone numbers where they were sent to. The “View Available OTC” allows the administrator to return to the list of unassigned OTCs.

The third enrollment method allows the end user to directly enroll his mobile phone through the Endpoint Protector Cloud Service, which can be accessed at two separate links, one for each supported mobile device operating system. This option requires the user to previously receive the MDM ID and OTC keys from the administrator. In this case, the administrator must reserve one OTC from the list for the user making the request either by:

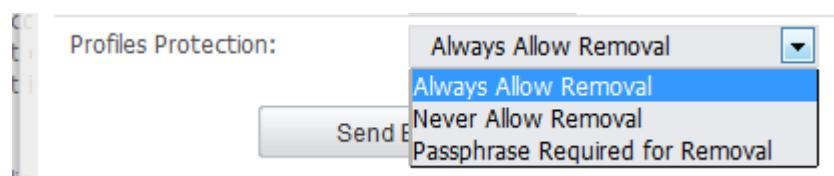
- using the “Reserve” right-click menu option 

This operation will remove the selected OTC from the list of the available OTCs and move it to the list of already sent invitations.

7.2.1. iOS and OS X Enrollment and Profile Protection

When an iOS or OS X device is enrolled the Administrator has the option to protect the policy/settings (called Profiles on iOS and OS X) against uninstallation. When an iOS or OS X device is enrolled it receives first an enrollment profile which is responsible for the communication between the device and the Endpoint Protector Appliance. This enrollment profile is not protected against uninstallation but all additional profiles attached to the enrollment profile can be protected against uninstallation. This means the restriction profile cannot be uninstalled from the device without a passcode that is protecting it, but the enrollment profile can be uninstalled, which also will uninstall the restriction profile.

The Profile Protection options are:



- **Always Allow Removal** – which allows the user to remove a profile at any time.
- **Never Allow Removal** – which allows removal of the profiles only through the Endpoint Protector Appliance Administrator.

- **Passphrase Required for Removal** – which allows the device user to delete the profile after entering the passphrase for deletion.

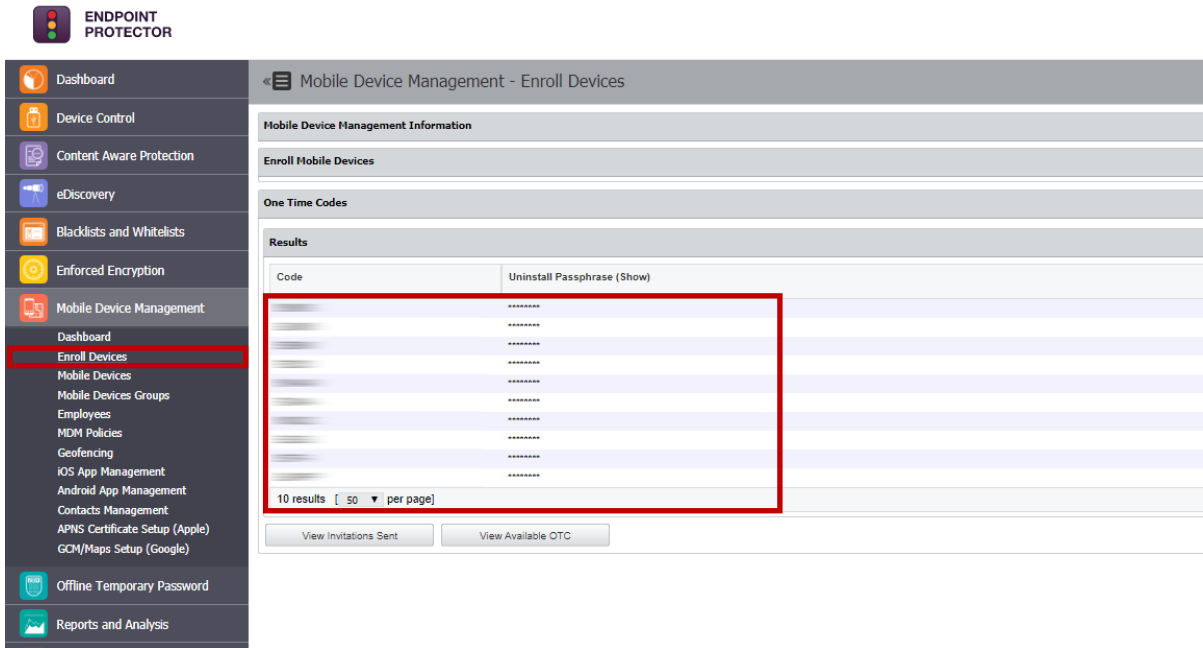
A practical example to illustrate this fact better is the following. An iPhone is enrolled and the administrator applies the companies' security policy for restrictions (disabling FaceTime for example) and Wi-Fi Settings as a profile and protects it with a profile protection. The user of the device wants to uninstall the restrictions profile to be able to use FaceTime. To do that the user is required to enter a passcode which he doesn't know (only the Endpoint Protector administrators). The user still could uninstall the enrollment profile (without a passcode) but in case he does that also all his other profiles and settings are deleted along with it, meaning company Wi-Fi settings etc.

7.2.2. iOS and OS X Profile Protection Deletion Passphrase

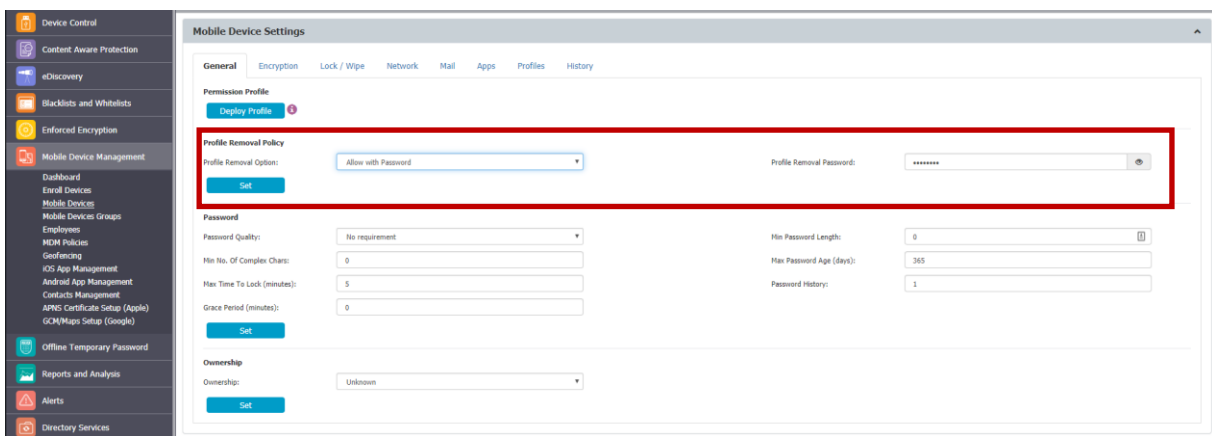
The passphrase for deletion of Profiles on iOS and OS X devices is by default generated randomly if during the invitation/enrollment process the Endpoint Protector Administrator who sends the invitation to the device sets the Profile Protection option to "Passphrase Required for Removal".

The automatically generated passphrase can be found in the Endpoint Protector Reporting and Administration web interface under Mobile Device Management > Enroll Devices > One Time Codes > Uninstall Passphrase(show).

After clicking on show the Passphrase is shown that corresponds to the device's enrollment OTC. In case the device user needs this passphrase, the administrator can give it to the user over the phone for the user to enter during deleting of a profile. The administrator can locate the Passphrase after clicking "View Invitations Sent" and locating the OTC used by the device for enrollment.



The Passphrase can also be set by the administrator manually under the option Mobile Device Management > Mobile Devices > General > Profile Removal Policy



7.2.3. Sending E-Mail or SMS Enrollment Invitation (iOS/OS X / Android)

Sending E-Mail or SMS enrollment invitations is made through the option “Enroll Devices”.

The screenshot shows a 'Send E-mail Request' dialog box. The 'Subject' field is 'Mobile Device Enrollment Request'. The 'Mobile Device Type' is 'iOS/Apple'. The 'Profiles Protection' dropdown menu is open, showing three options: 'Always Allow Removal' (selected), 'Never Allow Removal', and 'Passphrase Required for Removal'. A 'Send E-mail' button is visible below the dropdown.

Entering E-Mail and Phone numbers require attention to the correct format and selecting the device type, if known, in this step is of advantage due to a lesser chance that the user will select the wrong option.

For iOS and OS X devices in the device enrollment step as previously described it is important to set the Profile Protection settings.

7.2.4. SMS Enrollment Number Format (iOS / Android)

When sending SMS enrollment invitations, it is essential to send them using the correct number format.

The correct number format is: 401112345678

Country code, followed by area code and number, No + or zeroes are required in front of the country code.

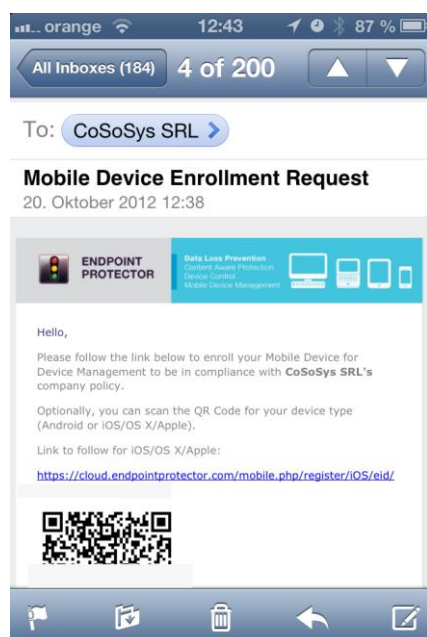
At all-time a country code is required, in case of US or Canadian numbers it is a 1, for Germany it is 49, etc.

7.2.5. E-Mail Enrollment Invitation (iOS/OS X / Android)

The device user can receive an enrollment invitation on the actual device and access the included URL (which includes already the MDM ID and OTC) to enroll the device.

Or if the e-mail is received with a desktop e-mail client, the user can scan the containing QR Code in the e-mail (which includes already the MDM ID and OTC) or access the included URL by typing it in the browser on the mobile device.

Below is shown an enrollment invitation e-mail on an iOS device.



In case the e-mail invitation is sent to an unknown device type it is important that the user chooses the proper device type from the available link options for iOS, OS X and Android devices.

7.2.6. SMS Enrollment Invitation (iOS / Android)

The device user should receive the enrollment invitation SMS on the actual device and access the included URL (which includes already the MDM ID and OTC) to enroll the device through the native browser of the device. In case of iOS it has to be accessed using Safari on the iPhone or iPad.

Below is shown an enrollment invitation SMS on an iOS device.



7.2.7. iOS and OS X Mobile Device Enrollment over URL

Note

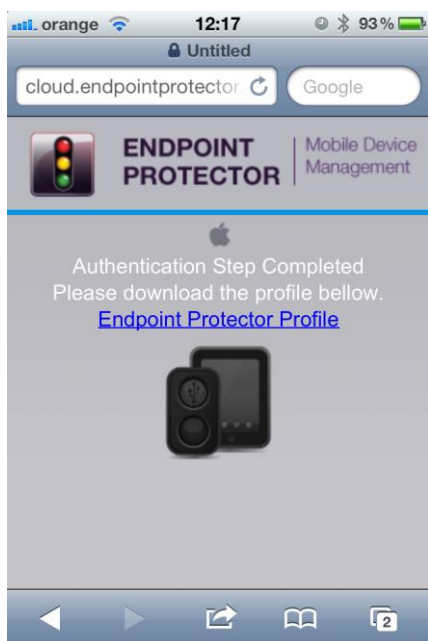
Enrollment of iOS devices should be done through the Safari browser on your iOS device or the iOS EPP MDM app from the App Store. Using other web browsers to enroll your iOS device is not supported.

The enrollment of an iOS or OS X device requires a working Internet connection (Wi-Fi or 4G/3G/2G). A 3G data connection is recommended for mobile devices. This way the communication with the Apple Servers can be performed and the information about the mobile device can be further transmitted to the Endpoint Protector Appliance/Server.

Once the user has received the invitation and clicked on the included link, a confirmation page will be displayed in his browser, auto-filled with the MDM ID and OTC keys.



After clicking on the "Connect" button, the user receives an Endpoint Protector profile for download, which must be further installed on his mobile device.



The user has to click on “Endpoint Protector Profile” to continue. The Profile has been generated at this step and is ready for installation.

Note

The profile is valid from this point on for two (2) hours. If the enrollment process is at this point interrupted for more than two hours the enrollment process has to be repeated from the start.

Next, the user must click on the “Install” button for the installation of the Endpoint Protector Profile.

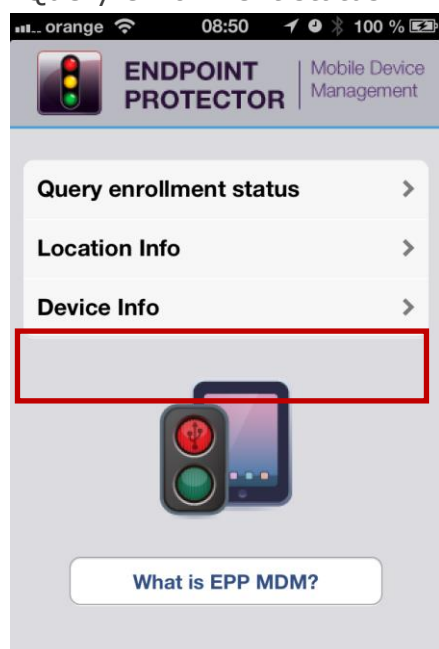


In case the iOS or OS X device has already a passcode/password set to access the device; the user is asked to access the passcode/password in order to confirm installation.

Once the Endpoint Protector Profile was successfully installed, the mobile device will be displayed inside the Mobile Devices List from the Endpoint Protector Web based Reporting & Administration Interface and it now available for the administrator to manage it.

7.2.8. iOS Mobile Device Enrollment through EPP MDM App

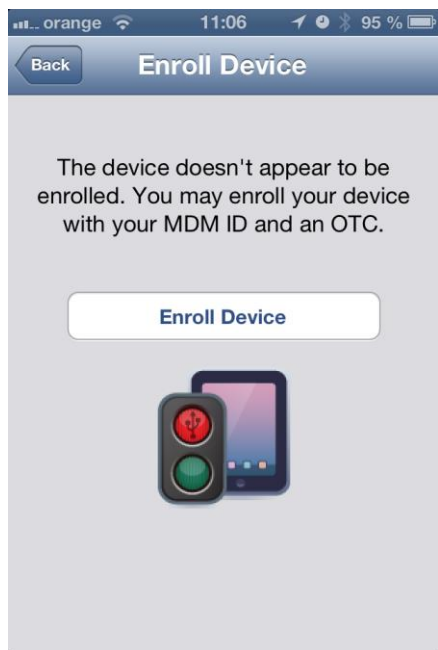
To enroll using the EPP MDM iOS app from the Apple App Store the user has to install the app on the iOS Device. After installing the EPP MDM iOS app (as described before in 5.5 Installing the EPP MDM iOS App) the user has to click “Query enrollment status”



The app is now checking if the iOS device is already enrolled with Endpoint Protector Mobile Device Management.

If the device is not enrolled yet the following message will appear “The device doesn’t appear to be enrolled....” If the device is enrolled already it will appear

“Device enrolled”.

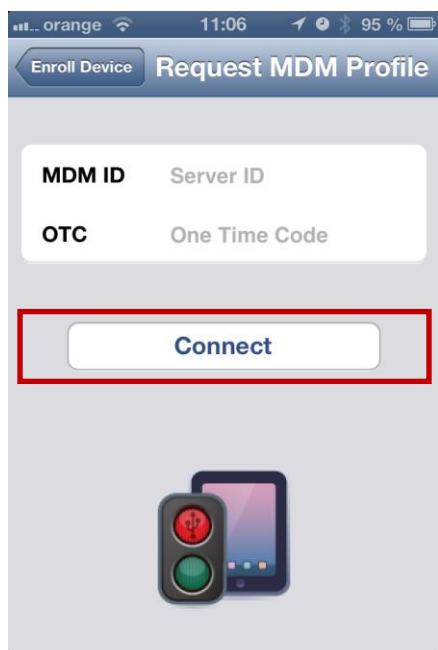


Left image, device not enrolled yet.

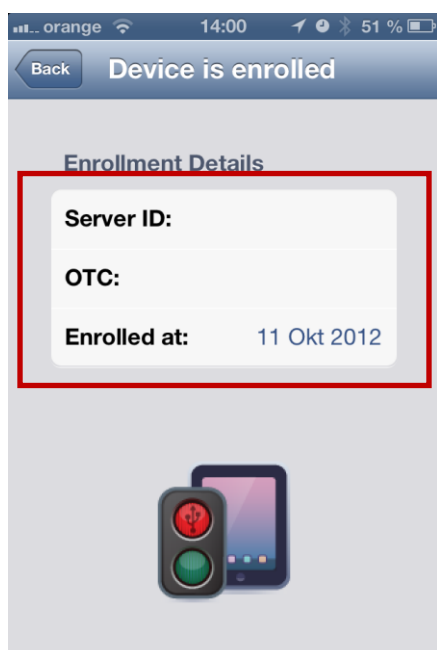


Right image, device is already enrolled.

In case the device is not enrolled yet click “Enroll Device” to continue.



Provide the MDM ID (MDM ID is located as described before 7.2) and an OTC (One Time Code) that is provided by the Endpoint Protector Administrator and click “Connect”.



After a device is successfully enrolled the Device enrolled status displays the MDM ID (Server ID) and OTC used along with the date when the device was enrolled.

7.2.9. Android Device Enrollment

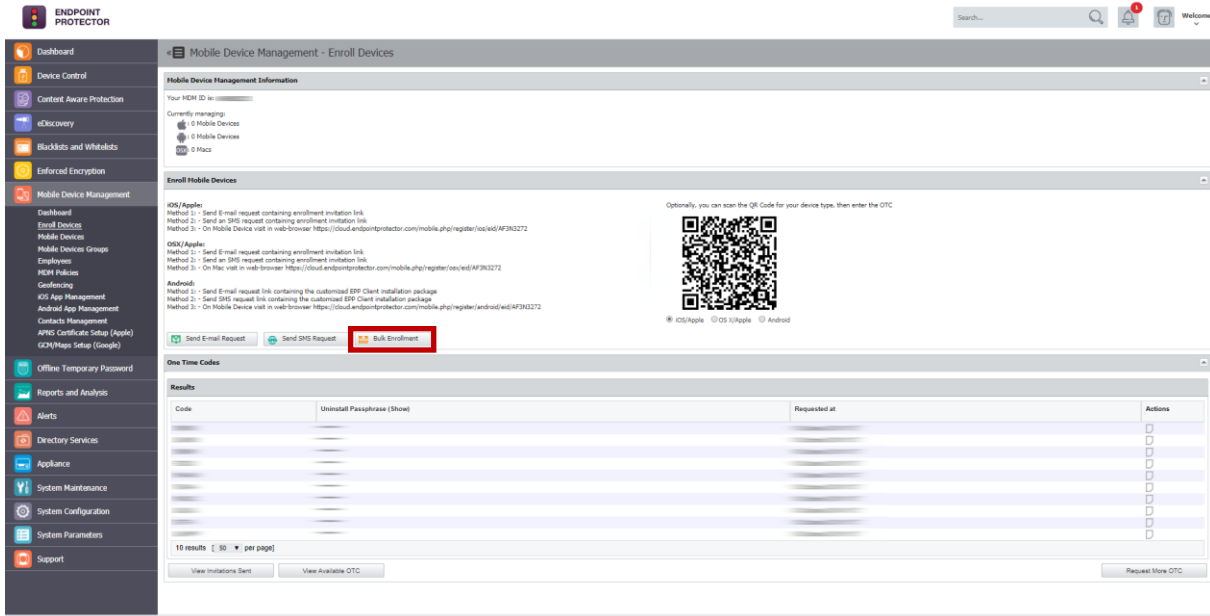
To enroll an Android mobile device, a Google Account is required to be previously setup by the user on the device. This is usually done when the user receives a new device and starts using it. Additionally, an Internet connection is mandatory for the communication between Endpoint Protector Appliance and the Android device. At least a 3G data connection is recommended to allow the communication with Google and Endpoint Protector Appliance and the transmission of the mobile device information.

Once the user has received the invitation and clicked on the included link, a confirmation page will be displayed in his browser, auto-filled with the MDM ID and OTC keys.

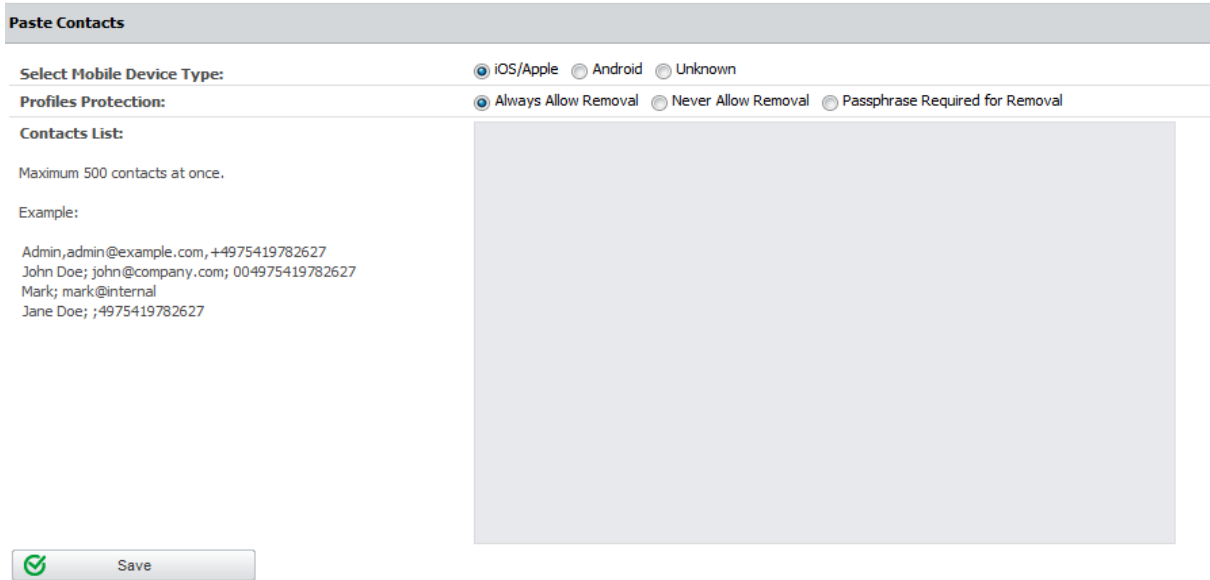
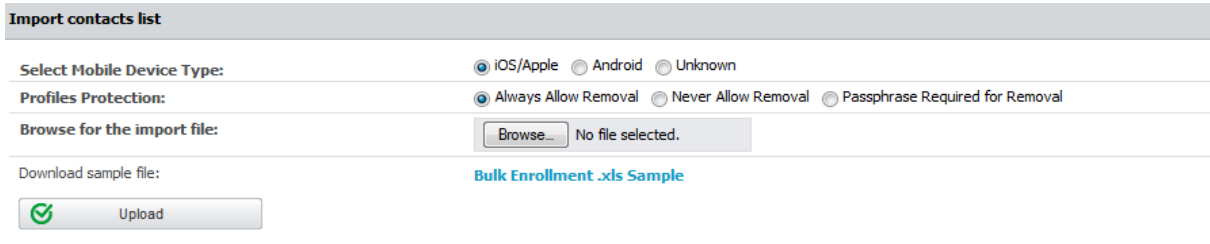
These steps are described in detail in chapter 6.4 Install EPP Client App on Android and Enrolling Android Device.

7.2.10. Bulk Enrollment

Bulk enrollment allows the administrator to send enrollment invitations to a large number of devices at the same time, through contacts list.



Contacts list can be imported from an .xls file or can be created in the „Paste Contacts“ section.



It is possible to paste up to 500 contacts at once. The required format is: name, separated with semicolon (;) the E-mail, separated with semicolon (;) the

Telephone Number. (Example John A. ; john@company.com ; country_prefix-xxxxxx). Please note that a „Bulk Enrollment .xls Sample“ file with a few examples inside is available for downloading.

Regardless of the way the contacts list is created, the mobile device type, and profile protection must be selected, otherwise a wrong enrollment link might be sent. Choose „Unknown“ at „Select Mobile Device Type“, if the devices to which the invitations will be sent are not just of one type(iOS, OS X or Android).

The added contacts will be available in the „Results“ section.

The screenshot shows the 'Results' section of the mobile device management interface. It features a table with the following columns: All, Type, Contact, E-mail, Phone, and Actions. The table contains four rows of contact information:

All	Type	Contact	E-mail	Phone	Actions
<input type="checkbox"/>	iOS	John A.	john@company.com	074xxxxxxx	
<input type="checkbox"/>	iOS	Mark B.	mark@company.com	074xxxxxxx	
<input type="checkbox"/>	iOS	Paul C.	paul@example.com	074xxxxxxx	
<input type="checkbox"/>	iOS	Dan D.	dan@example.com	074xxxxxxx	

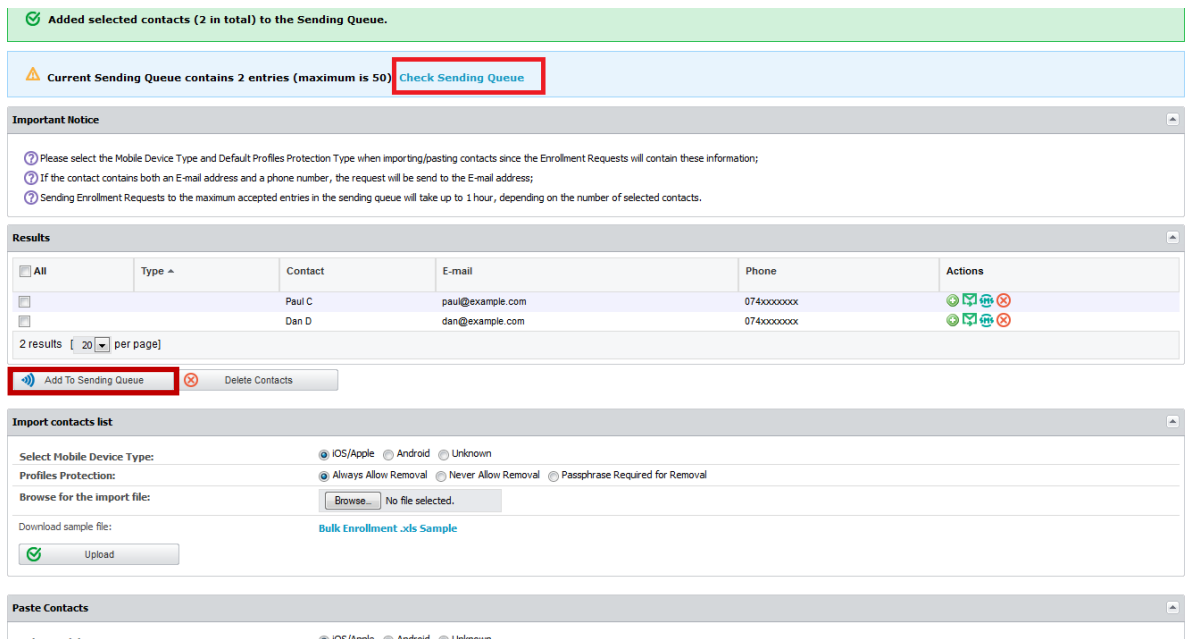
Below the table, there are buttons for 'Add To Sending Queue' and 'Delete Contacts'. The 'Add To Sending Queue' button is highlighted with a red box in the original image.

To add the selected contacts to the sending queue click on „Add To Sending Queue“ button.

This screenshot is similar to the one above, showing the 'Results' section. In this version, the 'Add To Sending Queue' button is highlighted with a red box, indicating the action to be taken. The table and other interface elements are identical to the previous screenshot.

In case both e-mail and telephone number is given, the enrollment invitation will be sent via e-mail. Sending all the invitations might take up to one hour, depending on the number of selected contacts.

To view the pending enrollments click on the „Check Sending Queue“ link.



Note! Contacts to which the invitations were already sent will no longer be available in the interface.




8. Managing Mobile Devices

The list of enrolled mobile devices and their status is available under Mobile Device Management -> Mobile Devices.

The screenshot displays the Endpoint Protector web interface. The left sidebar shows the navigation menu with 'Mobile Devices' highlighted under 'Mobile Device Management'. The main content area is titled 'Mobile Device Management - Mobile Devices' and contains a 'List of Mobile Devices' table. The table has columns for Mobile Device Name, OS Type, OS Version, Model, User, Mobile Phone, Carrier, Last Seen, Jailbroken/Routed, Status, and Actions. Three devices are listed: an iPhone 6 (Mobile Profiler Removed), a MacBook Pro (Registered), and a Samsung SM-G800P (Registered). Below the table are 'Enroll' and 'Delete' buttons. The top right of the interface includes a search bar, a notification bell, and a 'Welcome' dropdown.

Mobile Device Name	OS Type	OS Version	Model	User	Mobile Phone	Carrier	Last Seen	Jailbroken/Routed	Status	Actions
[Redacted]	iOS	12.4.1	iPhone6,2					No	Mobile Profiler Removed	[Edit] [Delete] [Refresh]
[Redacted]	OSX	10.14.5	MacBookPro15,1					No	Registered	[Edit] [Delete] [Refresh]
[Redacted]	Android	8.0.1	Samsung SM-G800P	Test	123	unknown		No	Registered	[Edit] [Delete] [Refresh]

To manage a specific device, select it from the list by right-clicking on the device name and choose one of the available actions: **Manage Device**, **Edit** and **Delete**.

-  Edit
-  Manage Settings
-  Delete

The **Edit** option allows the Administrator to list and edit details regarding the device and send a command to get latest details in real time.

Mobile Device Details	
Details	
Mobile Device Name:	iPhone 6 Test
OS Type:	iOS
Model:	iPhone 6
IMEI:	35 207506 896533 0
Mobile Phone:	Mobile Phone
Jailbroken:	No
Total Device Capacity:	115.19 GB
Battery Level:	21.00%
Last seen:	2019-10-23 13:16:56
Description:	Description
OS Version:	12.4.1
User:	User
WiFi:	34-A3-95-A3-3A-2A
Carrier:	Carrier
Supervised:	No
Available Device Capacity:	111.68 GB
Last iCloud Backup:	N/A
Status:	MobileProfileRemoved

The **Manage Setting** option allows the Administrator to manage an already enrolled device and enforce different settings to the device such as Lock/Wipe commands, Contact and Accounts management etc.

The **Delete** option once selected by the Administrator will delete a device and the corresponding history and logs from Endpoint Protector Appliance. We recommend not to “Delete” a device not before it was unmanaged. To unmanage a device, please check the section 15. Unmanage a Mobile Device in this manual.

8.1. Mobile Device Status

Mobile Device Name	OS Type	OS Version	Model	User	Mobile Phone	Carrier	Last Seen	Jailbroken/Routed	Status	Actions
	iOS	12.4.1	iPhone8					No	MobileProfileRemoved	
	OSX	10.14.5	MacBook Pro					No	Registered	
	Android	8.0.1	Samsung S9I-0800P	Test	123	unknown		No	Registered	

In the column Status the current mobile device status is shown if known to Endpoint Protector.

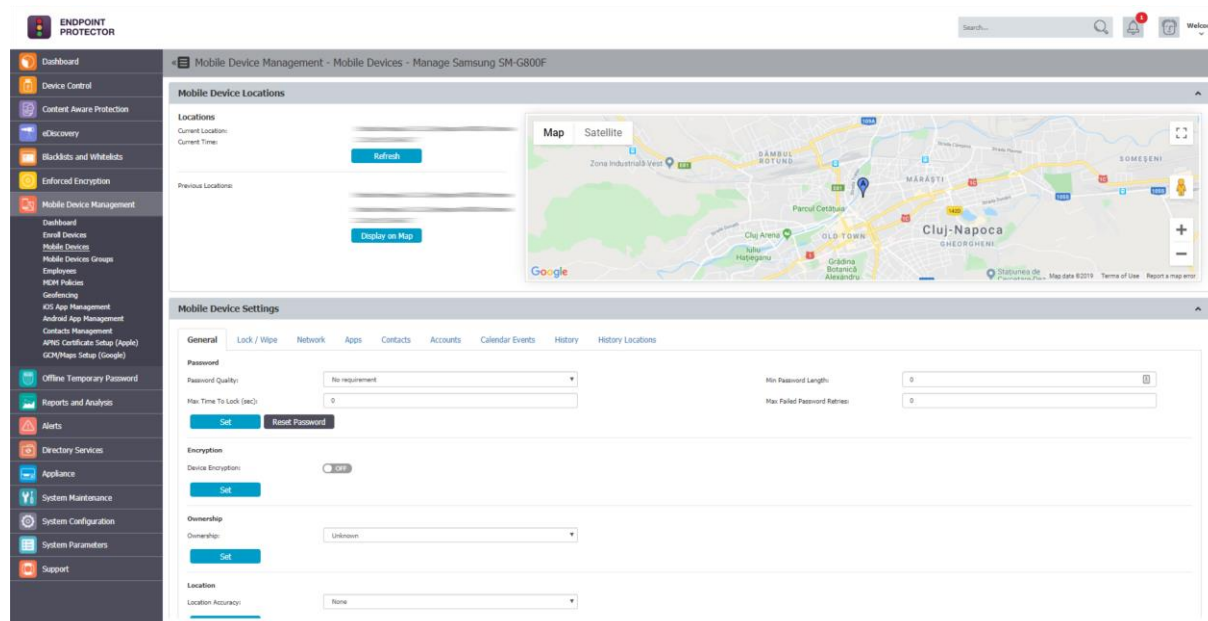
Registered – means the device is currently managed and Endpoint Protector MDM can communicate with the device. Applies to both iOS and Android devices.

MobileProfileRemoved – means the device is no longer managed. Either the device user has directly on the device removed the Enrollment Profile, or the Endpoint Protector Administrator has remotely removed the Enrollment Profile from the device to unmanage it. Applies to iOS devices.

DeviceAdminDisabled – means the device is no longer managed. Either the device user has directly on the device removed the EPP Client app, or the Endpoint Protector Administrator has remotely removed the EPP Client app from the device to unmanage it.

“Last Seen” is the time and date when the device has last time communicated with the Endpoint Protector MDM.

Selecting the “Manage Device” option for a mobile device will open the Manage Device page, containing different options to manage the selected device and to view information about it.


















The main three rows are the following three:

- Device Information:** displays all important device related details from mobile device name, model, type and OS to carrier related details such as carrier name, user phone number and user name. Not all information will be available all the time since the information available depends on the device and the operating system.
- Locate Device:** displays on the included map the previous and the current location of the device at the time of the last request. By selecting the “Update Location” option, the current location will be displayed on the map, while the “Location History” option will allow the Administrator to view the previous locations of the mobile device. For iOS only the current location is available of the device. For Android all location options are available, while for OS X there is no location information available. Please remember, iOS and Android both require for location information the EPP MDM app to be installed on the device.
- Device Management Tabs:** includes separate tabs containing the available MDM options for remote device and data managing. Detailed Features are described in the following paragraphs.

Available Options

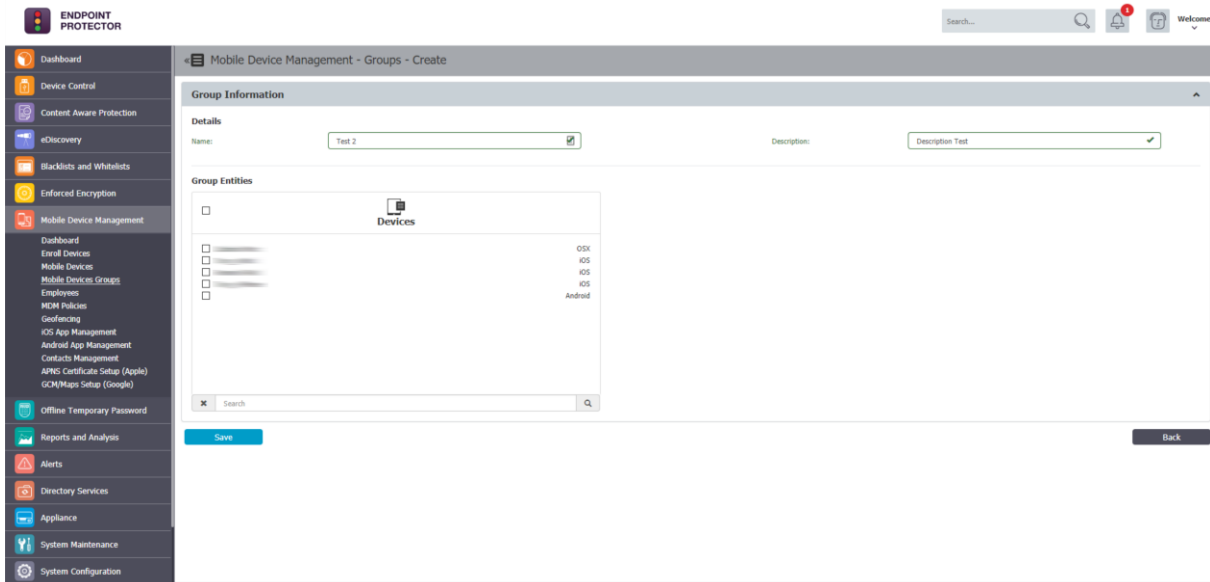
The table below shows the available MDM options for Android and iOS mobile Devices. More options will be made available updated with each version update.

Tab	MDM Option	Description	OS Support
Device Settings	Device Ownership	Allows to define the owner of the device: Personal, Company or Unknown	 /  / 
Device Settings	Voice Roaming	Allows to deactivate the Voice Roaming service for the mobile device (*Carrier dependent)	
Device Settings	Data Roaming	Allows to deactivate the Data Roaming service for the mobile device	
Device Settings	Device Location Settings	Allows to set additional parameters for the locating option: Location Accuracy Fine & Location Cost Allowed for a more accurate mobile device locating	 / 
Lock / Wipe	Lock Device	Remotely locks the user mobile device with or without resetting the user's password	 /  / 
Lock / Wipe	Wipe Device Data	Remotely deletes all device data. Additionally, the data stored on the SD Card can be deleted as well by checking the "Include SD Card" option	 /  / 
Lock / Wipe	Wipe SD Card	Remotely deletes all data stored on the SD Card	
Security Policy	Current Security Policy	Displays the security settings applied at that moment	 /  / 
Security Policy	File Vault 2 Disk Encryption	Encrypts the content of the disk automatically	
Security Policy	Set Security Policy	Allows defining additional password settings such as: minimum password length, password quality, max. time to lock, max. number of passwords retries before wipe.	 /  / 
Security Policy	Ask User to Change Password	Enforces the user to define a new password	 /  / 
Security Policy	Clear Password	Resets any existing password for the mobile device	
Security Policy	Device Password	Resets any existing password and allows defining remotely a different password for the mobile device	 /  / 

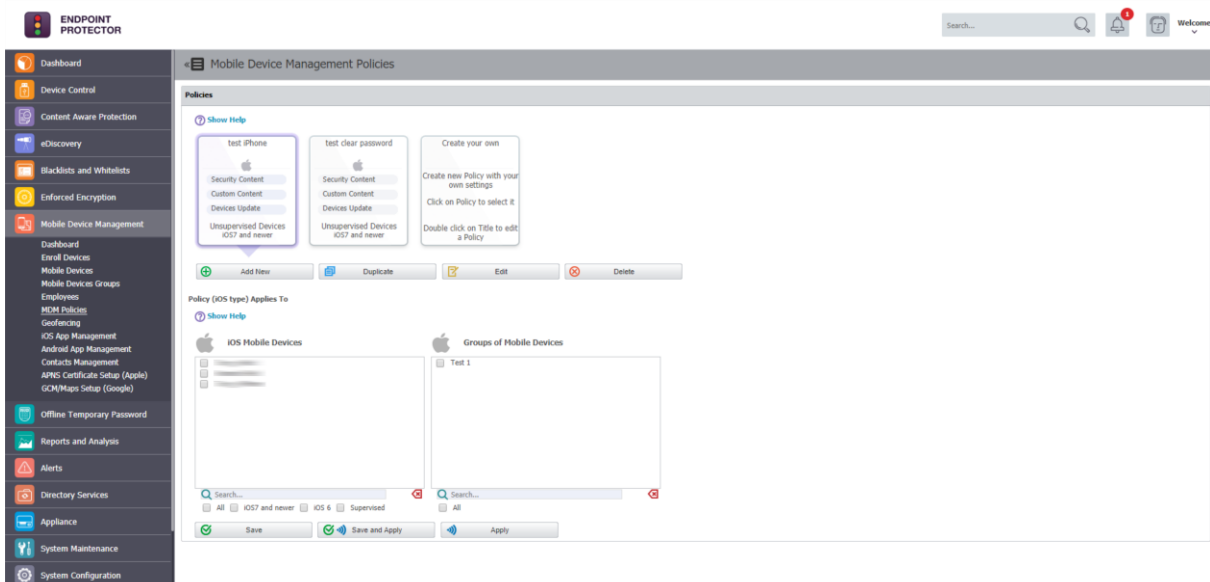
Manage Device	Refresh Device Details	Updates the device details displayed under Device Information	 /  / 
Manage Device	Refresh App List	Display the list of currently installed apps on the mobile device	 /  / 
Manage Device	Refresh Profile List	Display the list of currently set profiles on the mobile device	 / 
Manage Device	Refresh Google Accounts	Display the list of currently set Google e-mail accounts on the mobile device	
Manage Device	Refresh Accounts	Display the list of all currently set e-mail accounts on the mobile device	
Manage Device	Refresh Contacts	Display the list of all current contacts saved on the mobile device	
Installed Apps	Installed Apps	Shows the list of installed apps after selecting the Refresh Apps List option	 /  / 
Remove Installed Apps	Installed Apps	Removes the selected application from the list of installed apps and uninstalls the application from the mobile device	
Accounts	Accounts	Shows the list of e-mail accounts after selecting the Refresh Accounts / Refresh Google Accounts option	
Contacts	Contacts	Shows the list of contacts after selecting the Refresh Contacts option	
Profiles	Profiles	Shows the list of set profiles after selecting the Refresh Profile List option	 / 
History	History	Logs all device activity	 /  / 

8.2. Mobile Devices Groups

The Mobile Devices Groups section allows the creation of groups according to various needs. The search box also gives the end user the ability to more easily find devices.



Once the group is created, the end user can apply various policies to the newly created group, available in the „Groups of Mobile Devices“ section in the MDM Policies sub-menu.

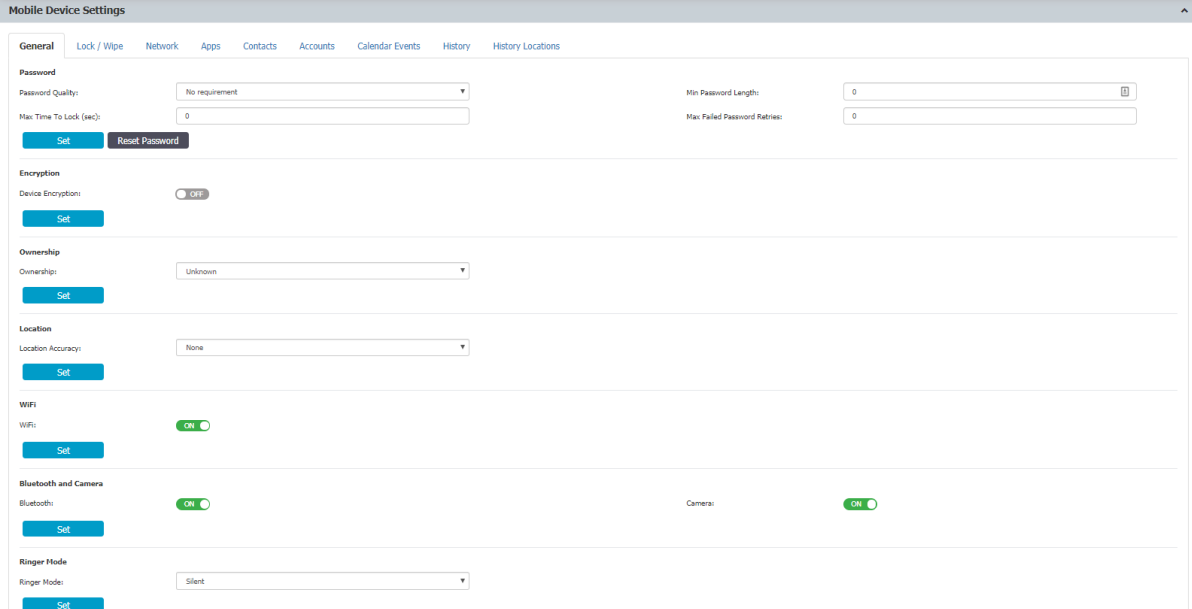


9. Manage iOS Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. For iOS the different management settings are stored as different profiles. One iOS device can have multiple profiles stored on it.

9.1. Security Settings (Security Profile) on iOS

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protecting your iOS devices.



The screenshot displays the 'Mobile Device Settings' interface for an iOS device. The settings are organized into several sections, each with a 'Set' button:

- General:** Includes tabs for Lock / Wipe, Network, Apps, Contacts, Accounts, Calendar Events, History, and History Locations.
- Password:** Features a 'Password Quality' dropdown menu set to 'No requirement', a 'Max Time To Lock (sec)' input field set to '0', a 'Min Password Length' input field set to '0', and a 'Max Failed Password Retries' input field set to '0'. There are 'Set' and 'Reset Password' buttons.
- Encryption:** Shows 'Device Encryption' as 'OFF' with a toggle switch and a 'Set' button.
- Ownership:** Shows 'Ownership' as 'Unknown' with a dropdown menu and a 'Set' button.
- Location:** Shows 'Location Accuracy' as 'None' with a dropdown menu and a 'Set' button.
- WiFi:** Shows 'WiFi' as 'ON' with a toggle switch and a 'Set' button.
- Bluetooth and Camera:** Shows 'Bluetooth' and 'Camera' as 'ON' with toggle switches and 'Set' buttons.
- Ringer Mode:** Shows 'Ringer Mode' as 'Silent' with a dropdown menu and a 'Set' button.

9.1.1. Password / Passcode Setting on iOS Device

Mobile Devices > Security Policy > Set Security Policy

The following Settings can be applied for the password / passcode settings for an iOS device:

- **Simple Value** – Example Password could be 1221
- **Alphanumeric Password** – Example could be 123A
- **Min Password Length** – Minimum number of digits
- **Min Number of Complex Chars** – Minimum number of complex characters. Complex characters are for example: !@#%&* etc.
- **Max Password Age (days)** – Number of days for which a user can use the same password. After that the user is requested to change the password to a new password.
- **Max Time to Lock (minutes)** – If iOS device is not used the device will lock (request password to access again) after set number of minutes.
- **Password History** – When a new password is set a new password is required. For example, if set to two, it means that after changing the password the user cannot reuse a previously used password until he has set two new passwords in the meantime.
- **Grace Period (minutes)** – Means the time a user has to make a change to the password or to initially set a password after the device receives the security policy.
- **Max Failed Password Retries** – Means the number a user can enter a wrong password until the device will wipe all data and reset itself. In case of reset, the device is wiping its entire data and is reset to a factory default. All data on the device is erased and cannot be recovered.

9.1.2. Clear Passcode (No more password required)

Using the option “Clear Passcode” the current device password will be set to be empty; hence the device can be unlocked without entering a password. This feature can be helpful in case the device is damaged and a password cannot be entered through the device itself.

9.1.3. iOS Device Hardware Encryption

When the password/code for an iOS device is set the iOS, device is automatically using its built-in hardware encryption in order to protect data on the device in

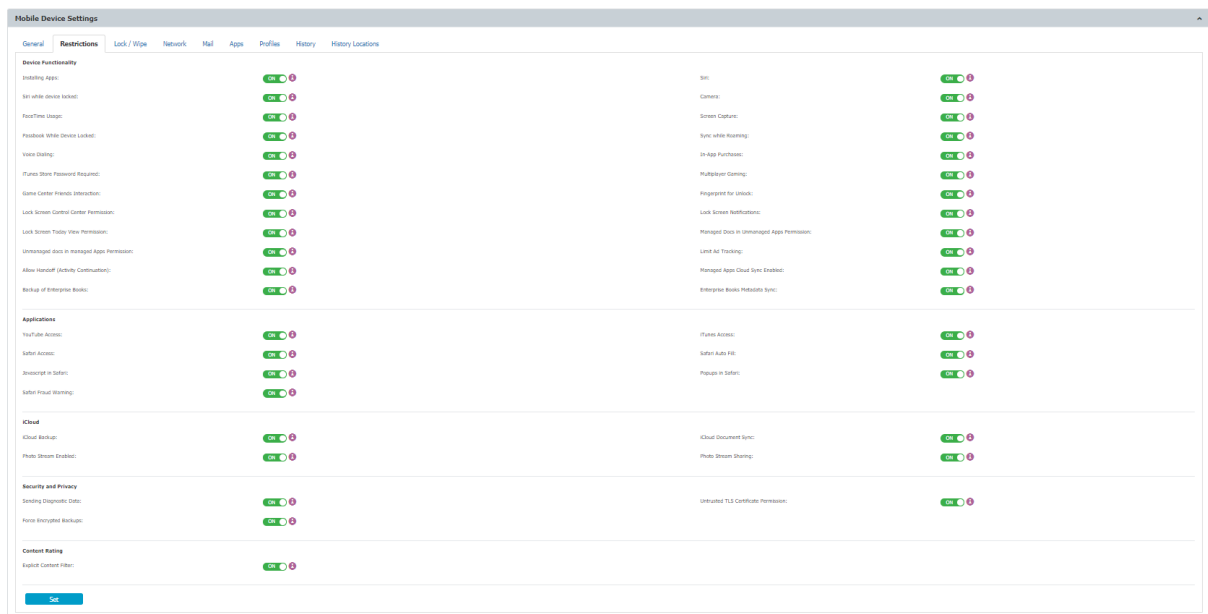
case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection.

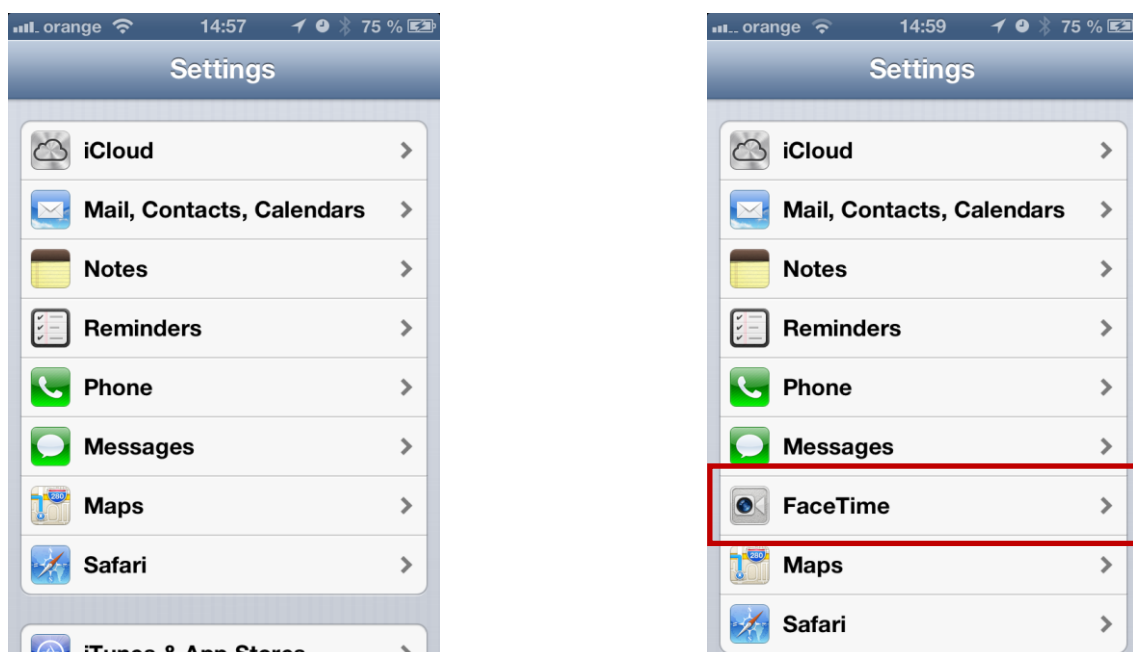
9.2. Restrictions (Restrictions Profile) on iOS

Mobile Devices > Security Policy > Set Restriction Policy

In order to use an iOS according to a company policy the Endpoint Protector Administrator can choose what options / features to allow to be used on the iOS device or to be disabled.

Disabling an option / feature will result in the option / feature being disabled from the iOS device. A practical example would be for the Administrator to disable the use of FaceTime. After the restriction policy is received by the iOS device, the FaceTime app icon and all FaceTime related options under Settings are removed (see screenshots below). The iOS device user has no option anymore to access or use the FaceTime feature.





Left image, FaceTime disabled (missing) by policy. Right image, FaceTime enabled without policy.

9.2.1. The following iOS features can be restricted

- Allow installing apps
- Allow Siri
 - Allow Siri while device locked
- Allow use of camera
- Allow FaceTime
- Allow screen capture
(making screenshots feature, holding home button and ON/OFF button to capture screen)
- Allow Passbook while device locked
- Allow sync while roaming
- Allow voice dialing
- Allow In-App Purchase
- Require iTunes Store password
- Allow multiplayer gaming
- Allow adding Game Center friends

9.2.2. The following Applications can be restricted

- Restrict YouTube App (native iOS YouTube)
Since YouTube is not part of iOS 6 anymore this feature is only supported for iOS 4 and iOS 5.
- Allow iTunes
- Allow Safari
- Allow Safari Auto Fill
- Allow JavaScript on Safari
- Allow popups on Safari
- Safari fraud warning

9.2.3. iCloud restrictions / Photo stream restrictions

iCloud is a service where almost all data on an iOS device is uploaded to Apple Servers. Some companies might choose to restrict the use of iCloud due to regulatory requirements, compliance requirements, data protection concerns or simply privacy concerns.

- Allow iCloud backup
- Allow iCloud document sync
- Allow photo stream
- Allow shared photo streams
Disallow photo stream can cause loss of data that was part of photo stream.

9.2.4. Security and Privacy Restrictions

- Allow sending diagnostic data
- Allow untrusted TLS certificate
- Force encrypted backups (when backing up iOS device to a computer)

9.2.5. Content Rating Restrictions

- Allow explicit content

9.2.6. iOS7 Restrictions

- Allow fingerprint for unlock
- Allow Lock Screen Control Center
- Allow Lock Screen Notifications
- Allow Lock Screen Today View
- Allow managed docs in unmanaged Apps
- Allow unmanaged docs in managed Apps
- Allow OTA PKI updates
- Limit ad tracking

9.2.7. Supervised Device Restrictions

- Allow AirDrop
- Allow Account Modification
- Allow App Cellular Data Changes
- Allow User Generated Siri Content
- Allow changes to Find My Friends
- Allow Host Pairing
- Allow iBookstore
- Allow Game center
- Allow iMessage
- Allow App Removal

9.3. Remote iOS Lock of Device

Mobile Devices > Lock / Wipe > Lock Device

The screenshot shows the 'Mobile Device Settings' interface. The 'Lock / Wipe' tab is selected. Under the 'Lock' section, the 'Lock:' dropdown menu is set to 'Lock', and there is a blue 'Set' button below it. Under the 'Wipe' section, the 'Wipe:' dropdown menu is set to 'Phone', and there is a blue 'Set' button below it.

The iOS device can be remotely locked. Clicking “Lock” will remotely lock the device screen and require a password entry to unlock the screen. The current password is kept in this case if the device is remotely locked.

The remote lock of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote locking of the device will still work as long as the lock command can reach the device.

9.4. Remote iOS Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data

The screenshot shows the 'Mobile Device Settings' interface with the 'Wipe' dropdown menu open. The 'Wipe:' label is followed by a dropdown menu showing three options: 'Phone', 'Phone & SD Card', and 'Phone & SD Card'. A blue 'Set' button is located below the dropdown menu.

The iOS device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device, click “Wipe” and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

After a remote wipe the device is unmanaged. No more connection between the iOS device and Endpoint Protector is possible after the remote wipe.

The remote wipe of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote wipe of the device will still work as long as the wipe command can reach the device.

Note

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort.

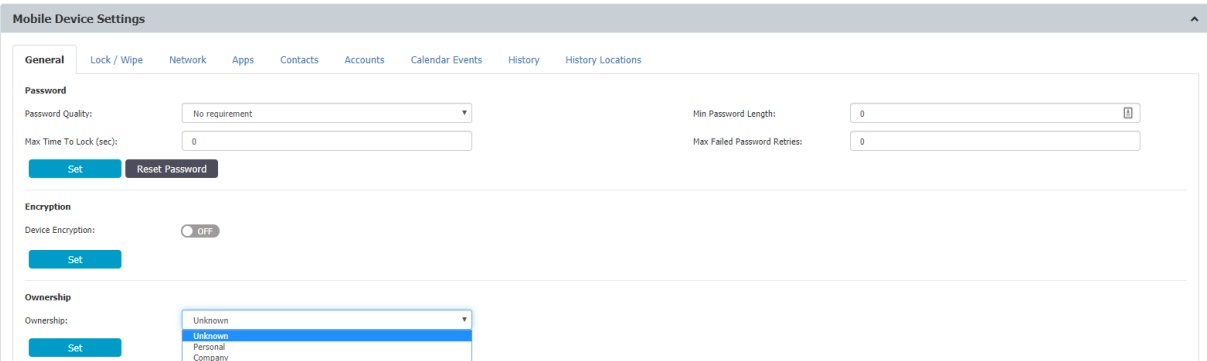
9.5. iOS Disable Device Password / Passcode

Mobile Devices > Security Policy > Clear Password (No more password required)

The option “Clear Password (No more password required)” will disable the password / passcode requirement for the iOS device. Unlocking the device screen will be possible without a password entry.

9.6. Device Ownership

Mobile Devices > Device Settings > Device Ownership



The screenshot displays the 'Mobile Device Settings' window with the 'General' tab selected. The 'Password' section includes a dropdown for 'Password Quality' (set to 'No requirement'), a 'Max Time To Lock (sec)' field (set to 0), a 'Min Password Length' field (set to 0), and a 'Max Failed Password Retries' field (set to 0). The 'Encryption' section shows 'Device Encryption' as 'OFF'. The 'Ownership' section has a dropdown menu with 'Unknown' selected, and other options are 'Unknown', 'Personal', and 'Company'. Each section has a 'Set' button.

The option “Device Ownership” can be set to who is the rightful owner of a device. Set it to “Company” if the company has purchased the device for the user or to “Personal” if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is set to “Unknown”.

9.7. Voice Roaming on iOS

Mobile Devices > General > Roaming

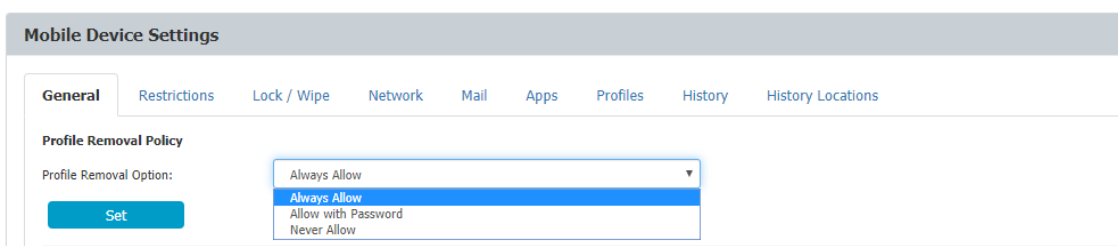


The option “Voice Roaming” can be set to allow a device to have voice roaming enabled while outside of range of the default cellular network. This setting can in some cases also be dependent on the cellular network provider. It might be required depending on the cellular subscription if voice roaming has to be activated first for the subscription before it can be enabled or disabled through Endpoint Protector.

The option “Data Roaming” can be set to allow a device to have data roaming enabled while outside of range of the default cellular network. This setting can in some cases also be dependent on the cellular network provider. It might be required depending on the cellular subscription if data roaming has to be activated first for the subscription before it can be enabled or disabled through Endpoint Protector MDM.

9.8. Profile Removal Policy for iOS Devices

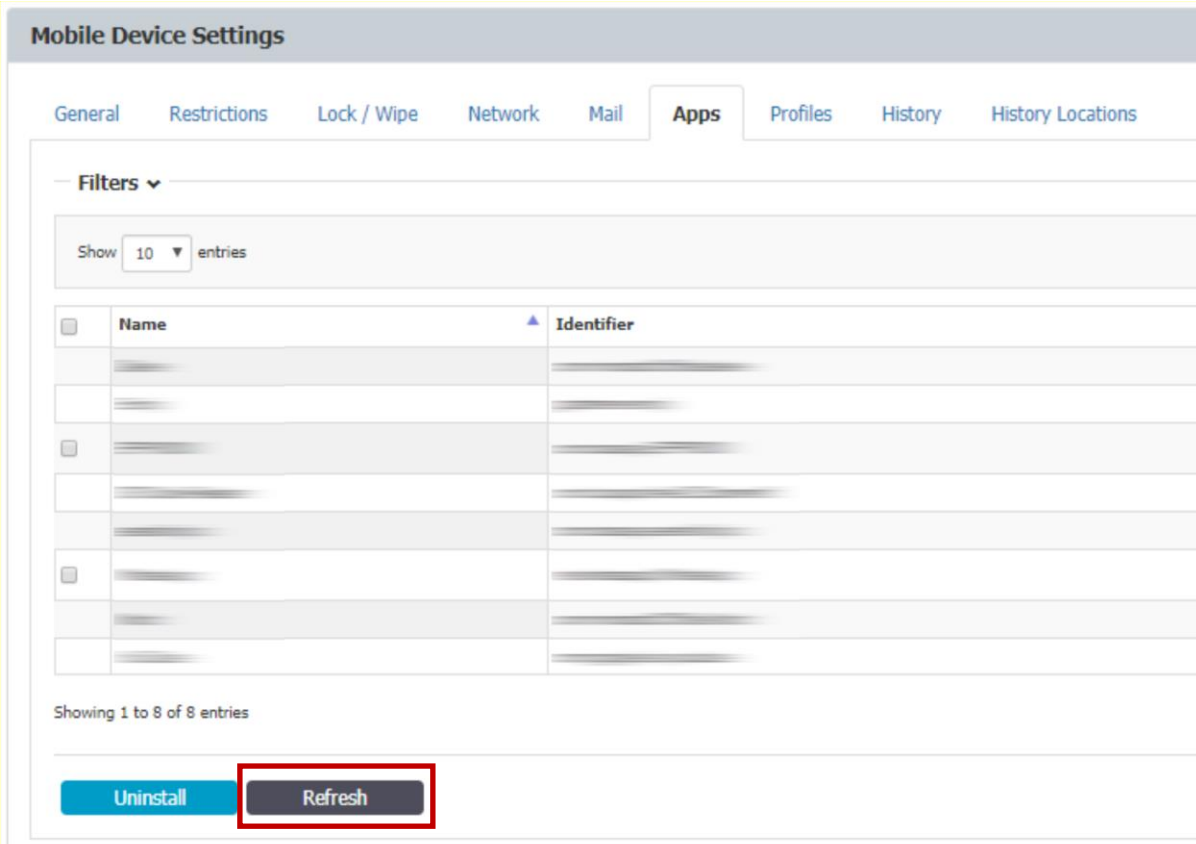
Mobile Devices > Manage Device > Profile Removal Policy



As described in the chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase before the profiles (settings) on an iOS Device can be protected with a passphrase. In this option the passphrase can be changed to be a different one than the one automatically generated and associated with the OTC. For the full description of this option please consult chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase.

9.9. Refresh App List for iOS

Mobile Devices > Manage Device > Refresh



The screenshot displays the 'Mobile Device Settings' interface with the 'Apps' tab selected. The interface includes a navigation bar with tabs for General, Restrictions, Lock / Wipe, Network, Mail, Apps, Profiles, History, and History Locations. Below the navigation bar, there is a 'Filters' section with a dropdown arrow and a 'Show 10 entries' control. The main content area features a table with two columns: 'Name' and 'Identifier'. The table contains several rows of data, with some rows having checkboxes in the 'Name' column. At the bottom of the table, there is a status bar that reads 'Showing 1 to 8 of 8 entries'. Below the status bar, there are two buttons: 'Uninstall' (blue) and 'Refresh' (grey). The 'Refresh' button is highlighted with a red rectangular box.

This function by clicking "Refresh" will ask the iOS device for a list of all the apps installed on the iOS device. The list of all installed Apps is shown in Endpoint Protector MDM at Mobile Devices > Installed Apps. If the user installs a new application, the list of the installed apps will be updated next time when the administrator will request the list of apps by pressing the "Refresh" button.

9.10. Installed Apps on iOS

Mobile Devices > Installed Apps

The List of Apps installed on the iOS device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the iOS device and updated through the option “Get Application List” as described in chapter 9.9

Filters

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

Name	Identifier	Version	Size	Status	Actions
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]

Showing 1 to 6 of 6 entries

Previous 1 Next

Uninstall Refresh

Installed Apps on managed iOS devices can be pushed, uninstalled and managed in different ways as described in the chapter 12 Mobile Application Management (MAM) for iOS.

9.11. Refresh Profile List on iOS

Mobile Devices > Manage Device > Refresh Profile List

Filters

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

Name	Identifier	Version	Size	Status	Actions
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]
-	-	-	-	Added	[trash icon]

Showing 1 to 6 of 6 entries

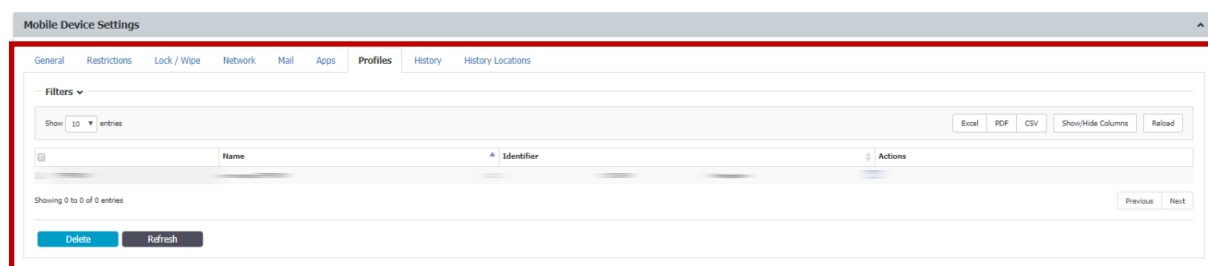
Previous 1 Next

Uninstall Refresh

The Profile List of an iOS device will show you what profiles are currently installed on the device. The list of installed profiles is shown here Mobile Devices > Profiles.


9.12. Profiles on iOS Devices Information

9.12.1. Mobile Devices > Profiles



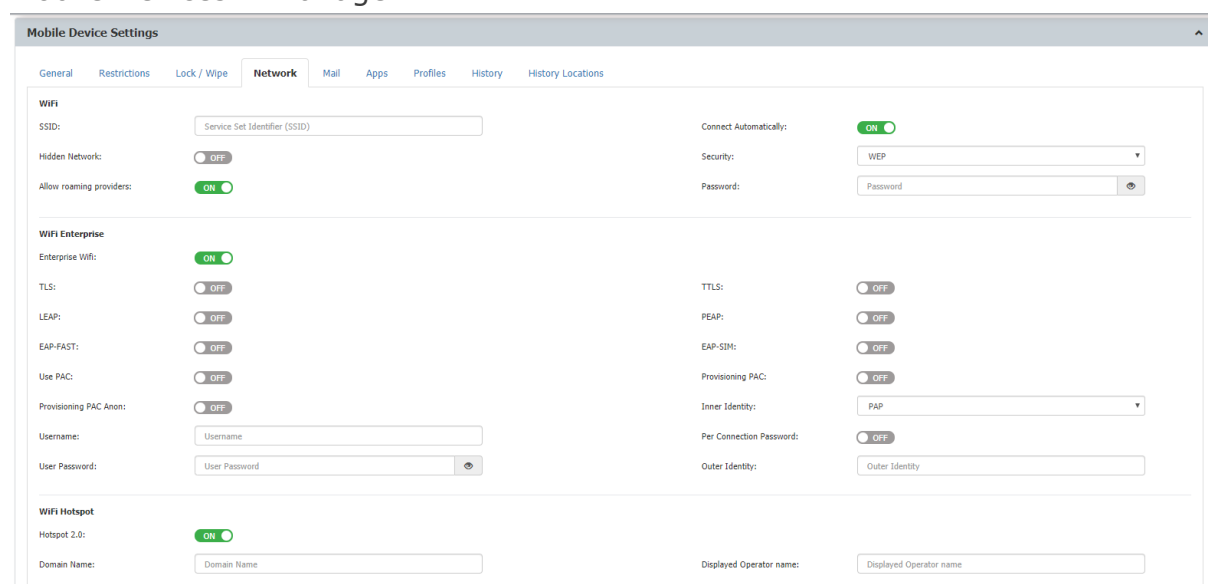
The profiles installed on an iOS Device are listed in the "Profile" tab. The Profiles installed on an iOS Device are always the enrollment Profile and possible restriction or other profiles. The type of profile is shown in the "Profile Description" column.

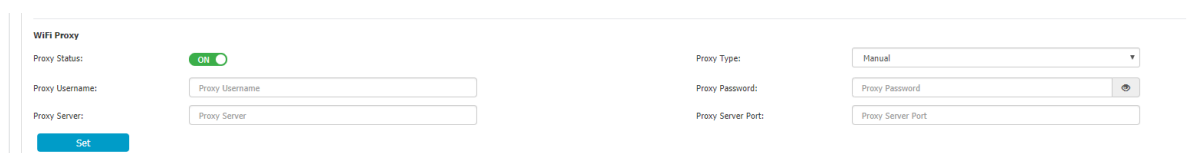
9.12.2. Remove Profile from iOS Device

From here the Endpoint Protector Administrator can also perform the remove action of a profile by clicking on  "Remove Profile". If a profile, e.g. a Restriction Profile is removed, the associated restrictions from the iOS device are removed. In case the Administrator want to unmanage a device, the Enrollment Profile needs to be removed. After removing the enrollment profile the device is no longer managed.

9.13. Manage Wi-Fi on iOS

Mobile Devices > Manage Wi-Fi





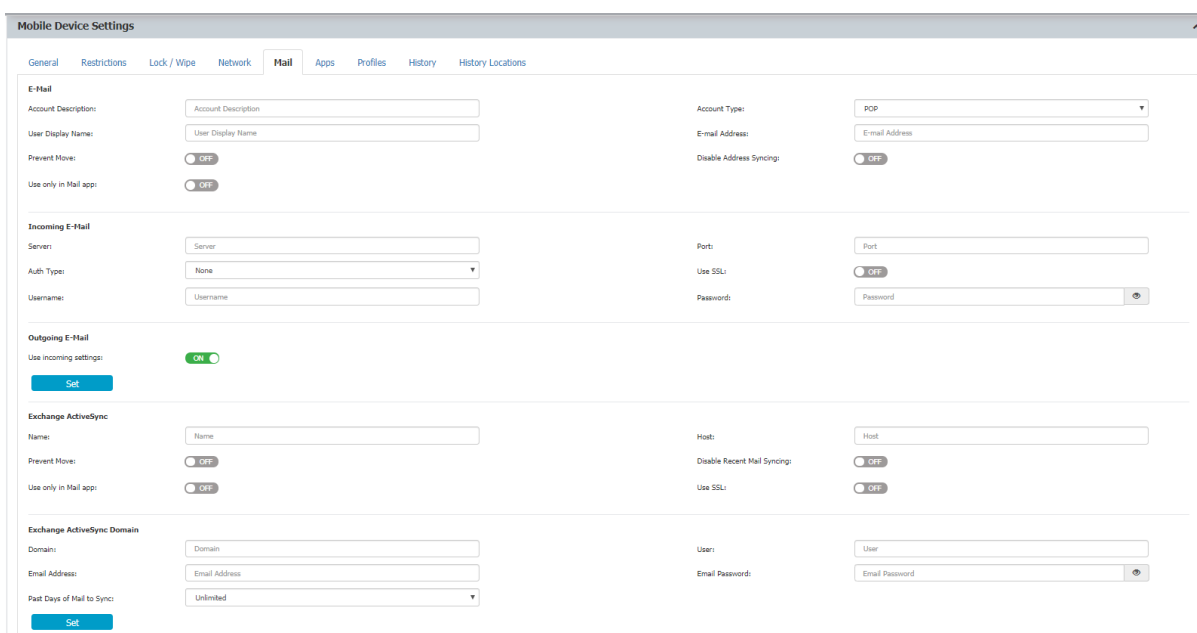
The Endpoint Protector Administrator can apply wireless network (Wi-Fi) settings to an iOS device. This can be used for iOS devices to automatically connect to a Wi-Fi access point without having to manually add the settings on the device.

9.13.1. Wipe Wi-fi Settings

Wi-Fi Profile can be removed to wipe company Wi-Fi Settings while personal Wi-Fi content remains untouched.

9.14. Manage Mail on iOS

Mobile Devices > Manage Mail



The Endpoint Protector Administrator can apply E-Mail settings to an iOS device. This can be used for iOS devices to automatically use company e-mail accounts and settings without having to manually add the settings on the device.

9.14.1. Wipe E-mail Settings

E-mail Profile can be removed to wipe company E-Mail Content and Settings while personal E-mail accounts and content remain untouched.

9.15. Manage VPN on iOS

Mobile Devices > Manage VPN

VPN	
Connection Name:	Connection 1
Provider:	Juniper SSL
Connection Type:	VPN
VPN Settings	
Route all traffic:	<input checked="" type="checkbox"/>
Server:	192.168.0.1
Account Name:	Username
Account password:	*****
Realm:	Realm 1
Role:	Role

The Endpoint Protector Administrator can apply VPN settings to an iOS device. This can be used for iOS devices to automatically deploy and use company VPN settings and policies without having to manually add the settings on the device.

9.16. Manage APN settings on iOS

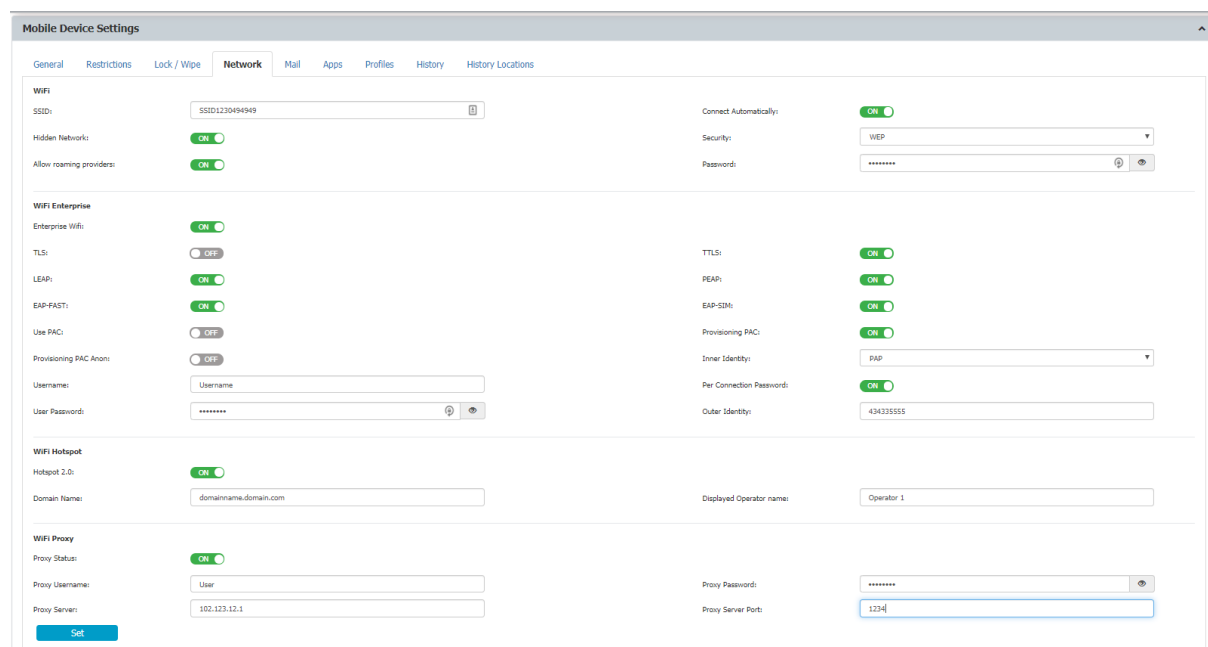
The Access Point Name (APN) defines the network path for all cellular data connectivity. You can view or edit the APN for cellular data services on iPhone or iPad, if your device uses a SIM card and your carrier allows you to edit the Access Point Name.

APN	
Name:	John Doe
Authentication Type:	EAP
Username:	Username
Password:	*****
Proxy:	132.312.2.2
Proxy Port:	4321
<input type="button" value="Set"/>	

To change the settings on the target device, complete the required fields. You'll have to provide a name, access point username and password and proxy server if needed. Pressing "Apply" will push the cellular settings to the device.

9.17. Manage Cellular Settings on iOS devices

Cellular data is used for data communication in cellular networks. It doesn't affect your ability to make or receive phone calls or to use Wi-Fi networks for Internet connectivity.



The screenshot displays the 'Mobile Device Settings' application with the 'Network' tab selected. The interface is organized into several sections:

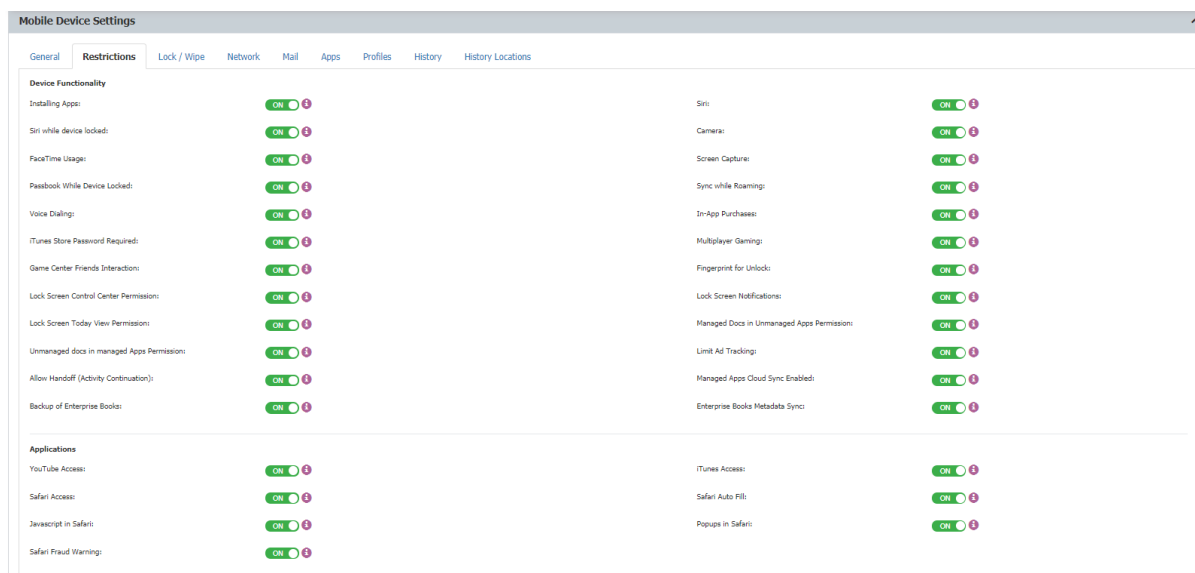
- WIFI:** Includes fields for SSID (SSID1230494949), Hidden Networks (ON), Allow roaming providers (ON), Connect Automatically (ON), Security (WEP), and Password (masked).
- WIFI Enterprise:** Includes Enterprise Wifi (ON), TLS (OFF), LEAP (ON), EAP-FAST (ON), Use PAC (OFF), Provisioning PAC Anon (OFF), Username (Username), User Password (masked), TLS (ON), PEAP (ON), EAP-SEM (ON), Provisioning PAC (ON), Inner Identity (PAP), Per Connection Password (ON), and Outer Identity (43433555).
- WIFI Hotspot:** Includes Hotspot 2.0 (ON) and Domain Name (domainname.domain.com).
- WIFI Proxy:** Includes Proxy Status (ON), Proxy Username (User), Proxy Server (102.123.12.1), Proxy Password (masked), and Proxy Server Port (1234).

A 'Set' button is located at the bottom left of the settings area.

To change the settings on the target device, complete the required fields. You'll have to provide a name, the authentication type, access point username and password and proxy server if needed. Pressing "Apply" will push the cellular settings to the device.

9.18. App Lock on iOS devices

The App Lock feature can be used to lock a device so only one application, which will be set from the server, can run on it. This feature is only available on Supervised iOS 7 devices.



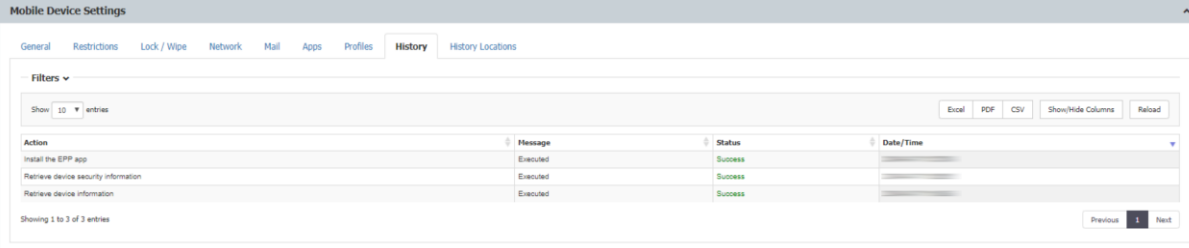
If the list of existing applications on the device was never updated on the server, it is a must to press the "Refresh" button from the Manage Device section as explained in paragraph 9.11, otherwise there will be no application listed in the "App Identifier" dropdown. However, it is recommended to use "Refresh" each time before the App Lock feature is used to refresh the available apps.

After interrogating the device for the available apps, it is possible to set some further options which will define the usability of the application. Finally pressing the "Apply" button will enforce the on the device.

9.19. History of iOS Devices Actions

Mobile Devices > History

In the "History" tab a record of actions sent to an iOS device are saved and the corresponding results are shown as well. The result can be executed, error, failed or pending.



The screenshot shows the 'Mobile Device Settings' interface with the 'History' tab selected. The table below displays the history of actions performed on mobile devices.

Action	Message	Status	Date/Time
Install the EPP app	Executed	Success	
Retrieve device security information	Executed	Success	
Retrieve device information	Executed	Success	

Showing 1 to 3 of 3 entries

9.20. Contacts and Accounts Tab on iOS Devices

Mobile Devices > Contacts

Mobile Devices > Accounts

The tabs “Contacts” and “Accounts” have no functionality associated with them for iOS and show “No Results”. This function is currently only supported for Android devices.

10. Manage OSX Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. For OS X the different management settings are stored as different profiles. One OS X device can have multiple profiles stored on it.

10.1. Security Settings (Security Profile) on OS X

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protect your OS X devices.

The screenshot displays the 'Mobile Device Settings' interface for OS X. It features a navigation bar with tabs: General, Encryption, Lock / Wipe, Network, Mail, Apps, Profiles, and History. The 'General' tab is active, showing the 'Permission Profile' section with a 'Deploy Profile' button. Below this is the 'Profile Removal Policy' section, which includes a dropdown for 'Profile Removal Option' (set to 'Allow with Password') and a 'Profile Removal Password' field. The 'Password' section contains several input fields: 'Password Quality' (set to 'Complex'), 'Min No. Of Complex Chars' (0), 'Max Time To Lock (minutes)' (5), 'Grace Period (minutes)' (0), 'Min Password Length' (0), 'Max Password Age (days)' (365), and 'Password History' (1). Each section has a 'Set' button. The 'Ownership' section at the bottom has a dropdown for 'Ownership' (set to 'Company') and a 'Set' button.

10.1.1. Password / Passcode Setting on OS X Device

Mobile Devices > Security Policy > Set Password Security Policy

The following Settings can be applied for the password / passcode settings for an OS X device:

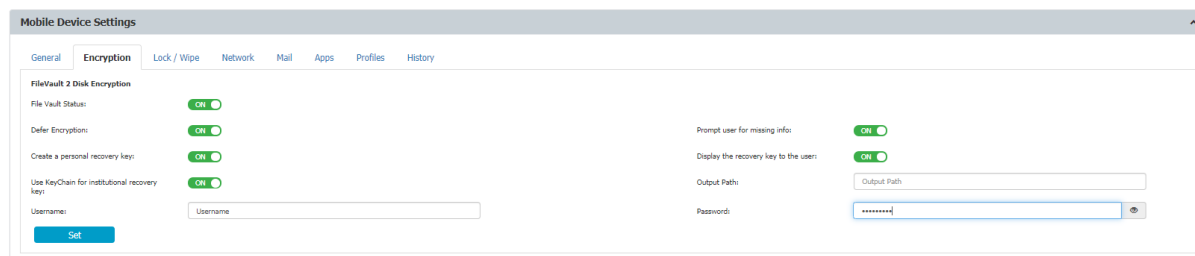
- **Simple Value** – Example Password could be 1221
- **Alphanumeric Password** – Example could be 123A
- **Min Password Length** – Minimum number of digits
- **Min Number of Complex Chars** – Minimum number of complex characters. Complex characters are for example: !@#\$%&* etc.
- **Max Password Age (days)** – Number of days for which a user can use the same password. After that the user is requested to change the password to a new password.
- **Max Time to Lock (minutes)** – If the OS X device is not used the device will lock (request password to access again) after set number of minutes.
- **Password History** – When a new password is set a new password is required. For example, if set to two, it means that after changing the password the user cannot reuse a previously used password until he has set two new passwords in the meantime.
- **Grace Period (minutes)** – Means the time a user has to make a change to the password or to initially set a password after the device receives the security policy.

10.1.2. OS X Device Hardware Encryption

When the password/code for an OS X device is set the OS X, device is automatically using it's built in hardware encryption in order to protect data on the device in case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection.

10.2. File Vault 2 Disk Encryption on OS X

With File Vault 2 you can encrypt the contents of your entire drive to help keep your data secure using XTS-AES 128 encryption.



Here are some guidelines on how to use the File Vault 2 Disk Encryption:

The first step is to change the “File Vault” dropdown to “On/Enable” status. Then there are a few options that can be selected below. Let’s take a walk through these buttons and see what each one means.

Defer Encryption – it will defer the encryption until the current user of the Mac will log out.

Prompt user for missing info - in case the administrator did not set the “Password”, it will prompt the user to complete, on the device, the missing info.

Create a personal recovery key - File Vault will create a personal key that can be used in case the user password on the device is lost or forgotten, and access is needed to the File Vault encryption.

Display the recovery key to the user – Before starting the encryption the recovery key will be shown to the user, so the user can save it/note it somewhere.

Use Keychain for institutional recovery key- An institutional key will be created and saved at `/Library/Keychains/FileVaultMaster.keychain`

Output Path – the location on the device where the personal recovery key will be saved

Username – must be an existing user that is already created on the target device

Password – the password for the user.

10.2.1. Disk Encryption Status

File Vault 2 Disk Encryption also has a Status field where it is possible to find information such as the Encryption Status, if the Personal Recover Key was defined or not and if the Institutional Recovery Key was defined or not.

10.3. Remote Lock of Device

Mobile Devices > Lock / Wipe > Lock Device

The screenshot shows the 'Mobile Device Settings' window with the 'Lock / Wipe' tab selected. Under the 'Lock' section, there is a dropdown menu labeled 'Lock' with a downward arrow, and a 'Set' button below it. To the right, there is a 'Lock PIN:' label followed by a text input field containing four asterisks. Under the 'Wipe' section, there is a dropdown menu labeled 'Wipe' with a downward arrow, and a 'Set' button below it. To the right, there is an 'Unlock PIN:' label followed by a text input field containing four asterisks.

The OS X device can be remotely locked and a PIN can be set. Clicking “Lock” will remotely lock the device screen and the user will have to enter the PIN to unlock it. The PIN must be a four (4) digit number.

10.4. Remote OS X Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data

This screenshot is identical to the one above, showing the 'Mobile Device Settings' window with the 'Lock / Wipe' tab selected. It displays the 'Lock' and 'Wipe' sections with their respective dropdown menus, 'Set' buttons, and PIN input fields.

The OS X device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device, click “Wipe” and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

After a remote wipe the device is unmanaged. No more connection between the OS X device and Endpoint Protector is possible after the remote wipe.

The “Find My Mac PIN” password protects the wiped device. After the device is wiped it will be locked and cannot be used unless the PIN is entered.

Note

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort, as all existing user's data will be wiped.

10.5. Device Ownership

Mobile Devices > Device Settings > Device Ownership

The screenshot shows the 'Ownership' settings. A dropdown menu is open, displaying the following options: 'Company', 'Unknown', 'Personal', and 'Company'. A blue 'Set' button is located below the dropdown.

The option “Device Ownership” can be set to who is the rightful owner of a device. Set it to “Company” if the company has purchased the device for the user or to “Personal” if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is “Unknown”.

10.6. Profile Removal Policy for OS X Devices

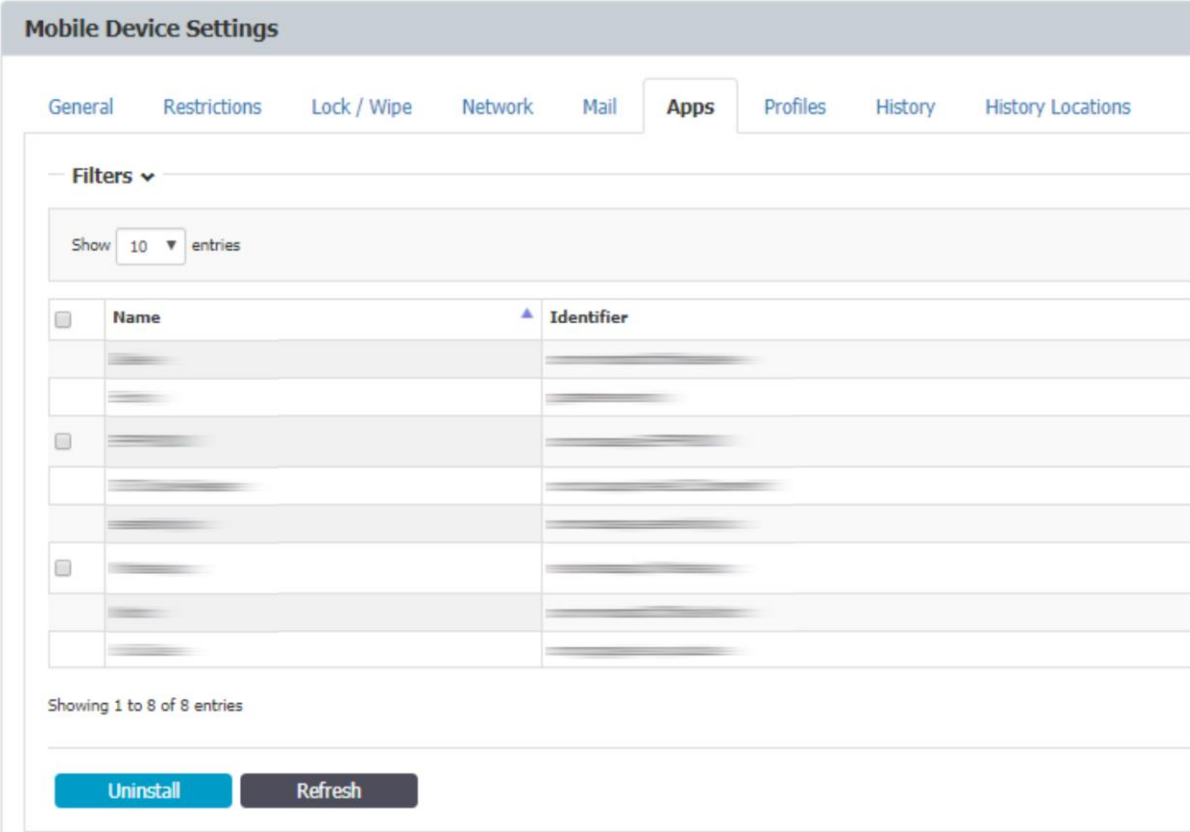
Mobile Devices > General > Profile Removal Policy

The screenshot shows the 'Mobile Device Settings' interface. The 'General' tab is selected. Under the 'Profile Removal Policy' section, a dropdown menu for 'Profile Removal Option' is open, showing the following options: 'Always Allow', 'Always Allow', 'Allow with Password', and 'Never Allow'. A blue 'Set' button is located below the dropdown.

As described in the chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase before the profiles (settings) on an OS X Device can be protected with a password. In this option the password can be changed to be a different one than the one automatically generated and associated with the OTC. For the full description of this option please consult chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase.

10.7. Refresh App List for OS X

Mobile Devices > Manage Device > Refresh



The screenshot displays the 'Mobile Device Settings' interface for an OS X device, specifically the 'Apps' tab. The interface includes a navigation bar with tabs for General, Restrictions, Lock / Wipe, Network, Mail, Apps (selected), Profiles, History, and History Locations. Below the navigation bar, there is a 'Filters' section with a dropdown arrow. A 'Show 10 entries' control is present. The main content area is a table with two columns: 'Name' and 'Identifier'. The table contains eight rows of data, each with a checkbox on the left. At the bottom of the table, there is a status indicator 'Showing 1 to 8 of 8 entries' and two buttons: 'Uninstall' (blue) and 'Refresh' (dark grey).

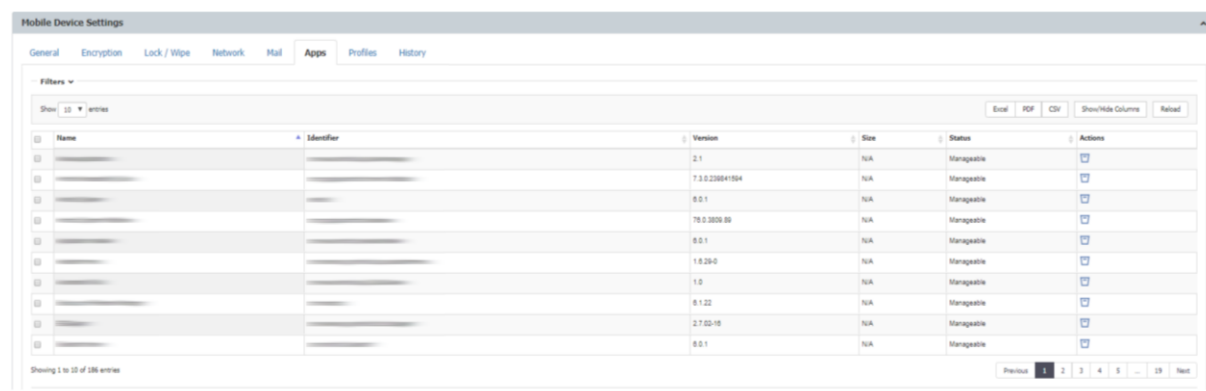
<input type="checkbox"/>	Name	Identifier
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]
<input type="checkbox"/>	[Redacted]	[Redacted]

This function by clicking "Refresh" will ask the OS X device for a list of all the apps installed on the OS X device. The list containing all installed applications will be shown at the "Installed Apps" section. If the user installs a new application, the list of the installed apps will be updated next time when the administrator will request the list of apps by pressing the "Refresh" button.

10.8. Installed Apps on OS X

Mobile Devices > Apps

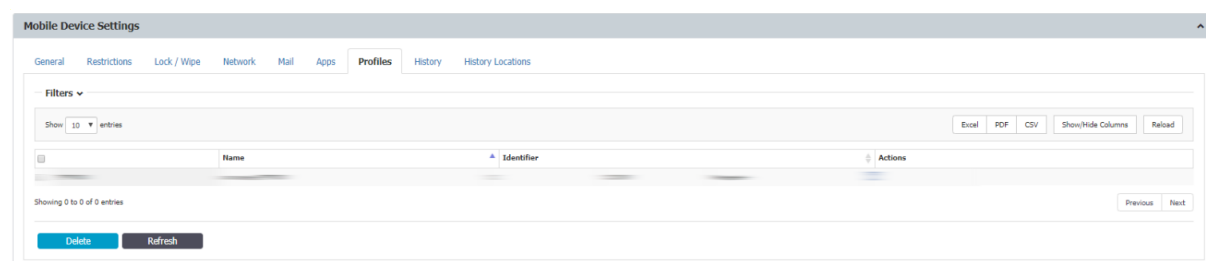
The list of Apps installed on the OS X device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the OS X device and updated through the option “Refresh”.



Name	Identifier	Version	Size	Status	Actions
		2.1	N/A	Manageable	
		7.3.0.238841554	N/A	Manageable	
		0.0.1	N/A	Manageable	
		78.0.3809.89	N/A	Manageable	
		0.0.1	N/A	Manageable	
		1.0.29-0	N/A	Manageable	
		1.0	N/A	Manageable	
		0.1.22	N/A	Manageable	
		2.7.02-10	N/A	Manageable	
		0.0.1	N/A	Manageable	

10.9. Refresh Profile List on OS X

Mobile Devices > Profiles > Refresh

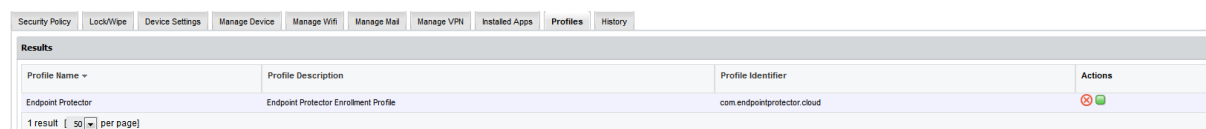


Name	Identifier	Actions
Showing 0 to 0 of 0 entries		

The Profile List of an OS X device will show you what profiles are currently installed on the device. The list of installed profiles is shown at Mobile Devices > Profiles.

10.10. Profiles on OS X Devices Information

Mobile Devices > Profiles




Profile Name	Profile Description	Profile Identifier	Actions
Endpoint Protector	Endpoint Protector Enrollment Profile	com.endpointprotector.cloud	⊗ ⊕

1 result (50 per page)

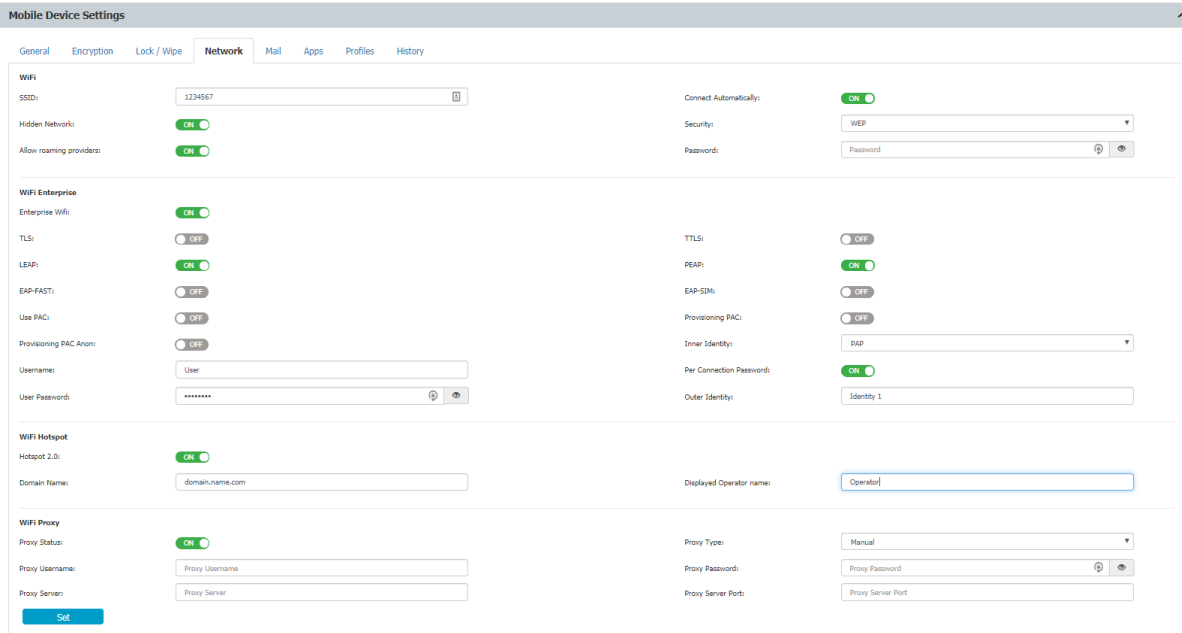
The profiles installed on an OS X Device are listed in the “Profiles” tab. There are two types of profile: the main Enrollment Profile and the restriction profiles. The type of profile is shown in the “Profile Description” column. If a new profile is installed on the device, the list of the installed profiles will be updated next time when the administrator will request the list of profiles by pressing the “Get Profiles List” button as described in paragraph 10.10.

10.10.1. Remove Profile from OS X Device

From here the Endpoint Protector Administrator can also perform the remove action of a profile by clicking on  “Remove Profile”. If a profile, e.g. a Restriction Profile is removed, the associated restrictions from the iOS device are removed. In case the Administrator want to unmanage a device, the Enrollment Profile needs to be removed. After removing the enrollment profile the device is no longer managed.

10.11. Manage Wi-Fi on OS X

Mobile Devices > Manage Wi-Fi



The screenshot shows the "Mobile Device Settings" window with the "Network" tab selected. The settings are organized into several sections:

- WiFi:** SSID (1234567), Hidden Networks (ON), Allow roaming providers (ON), Connect Automatically (ON), Security (WEP), Password (Password).
- WiFi Enterprise:** Enterprise WiFi (ON), TLS (OFF), LEAP (ON), EAP-FAST (OFF), Use PAC (OFF), Provisioning PAC Authn (OFF), Username (User), User Password (*****), TTLS (OFF), PEAP (ON), EAP-SIM (OFF), Provisioning PAC (OFF), Inner Identity (PAP), Per Connection Password (ON), Outer Identity (Identity 1).
- WiFi Hotspot:** Hotspot 2.0 (ON), Domain Name (domain.name.com), Displayed Operator name (Operator).
- WiFi Proxy:** Proxy Status (ON), Proxy Username (Proxy Username), Proxy Server (Proxy Server), Proxy Type (Manual), Proxy Password (Proxy Password), Proxy Server Port (Proxy Server Port).

A "Set" button is located at the bottom left of the settings area.

The Endpoint Protector Administrator can apply wireless network (Wi-Fi) settings to an OS X device. This can be used for OS X devices to automatically connect to a Wi-Fi access point without having to manually add the settings on the device.

10.11.1. Wipe Wi-fi Settings

Wi-Fi Profile can be removed to wipe company Wi-Fi Settings while personal Wi-Fi content remains untouched.

10.12. Manage Mail on OS X

Mobile Devices > Mail

The screenshot shows the 'Mobile Device Settings' window with the 'Mail' tab selected. The interface is divided into three main sections: E-Mail, Incoming E-Mail, and Outgoing E-Mail. Each section contains various configuration fields and toggle switches.

Section	Field Name	Value / Status
E-Mail	Account Description	E-mail Account 1
	User Display Name	John Doe
	Allow Moves	ON
	Use only in Mail app	ON
Incoming E-Mail	Server	192.123.12.12
	Auth Type	Password
	Username	User
	Port	1234
Outgoing E-Mail	Use incoming settings	ON
	Account Type	POP
	E-mail Address	email@email.com

Additional fields visible in the Incoming E-Mail section include 'Use SSL' (ON) and 'Password' (masked with asterisks). A 'Set' button is located at the bottom left of the configuration area.

The Endpoint Protector Administrator can apply E-Mail settings to an OS X device. This can be used for OS X devices to automatically use company e-mail accounts and settings without having to manually add the settings on the device.

10.12.1. Wipe E-mail Settings

E-mail Profile can be removed to wipe company E-Mail Content and Settings while personal E-mail accounts and content remain untouched.

10.13. Manage VPN on OS X

Mobile Devices > Network

The screenshot shows the 'Mobile Device Settings' window with the 'Network' tab selected. The interface is divided into three main sections: VPN, VPN Settings, and VPN Proxy. Each section contains various configuration fields and toggle switches.

Section	Field Name	Value / Status
VPN	Connection Name	Connection 1
	Connection Type	L2TP
VPN Settings	Authentication Type	Password
	Account Name	Account
	Route all traffic	ON
	Server	192.123.12.12
VPN Proxy	Proxy Status	ON
	Proxy Type	Manual
	Proxy Server	192.124.13.13
	Proxy Server Port	192.124.13.13

Additional fields visible in the VPN Settings section include 'Password' (masked with asterisks) and 'Shared Secret' (Shared Secret 1). A 'Set' button is located at the bottom left of the configuration area.

The Endpoint Protector Administrator can apply VPN settings to an OS X device. This can be used for OS X devices to automatically deploy and use company VPN settings and policies without having to manually add the settings on the device.

10.14. History of OS X Devices Actions

Mobile Devices > History

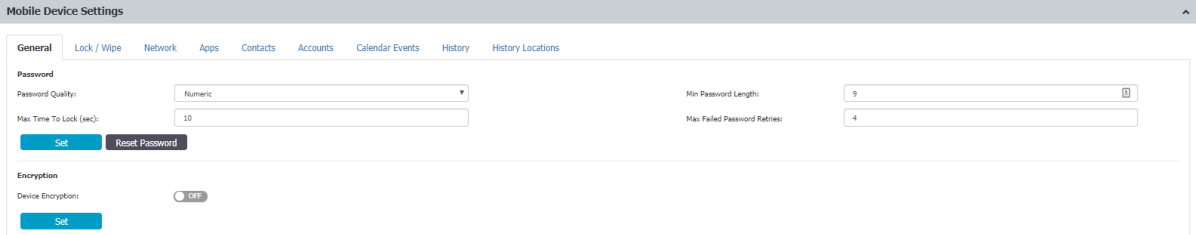
In the “History” tab a record of actions sent to an OS X device are saved and the corresponding results are shown as well. The result can be executed, error, failed or pending.

11. Manage Android Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. For Android the different management settings are enforced by the EPP Client on the Android device.

11.1. Security Settings (Security Profile) on Android

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protecting your Android devices.



The screenshot displays the 'Mobile Device Settings' window with the 'General' tab selected. The 'Password' section includes a dropdown for 'Password Quality' set to 'Numeric', a 'Max Time To Lock (sec)' field with '10', a 'Min Password Length' field with '9', and a 'Max Failed Password Retries' field with '4'. There are 'Set' and 'Reset Password' buttons. The 'Encryption' section shows 'Device Encryption' as 'OFF' with a 'Set' button.

The current Security Policy (if any) will be shown on under „Current Security Policy“.

11.1.1. Password / Passcode Setting on Android Device

Mobile Devices > Security Policy > Set Security Policy

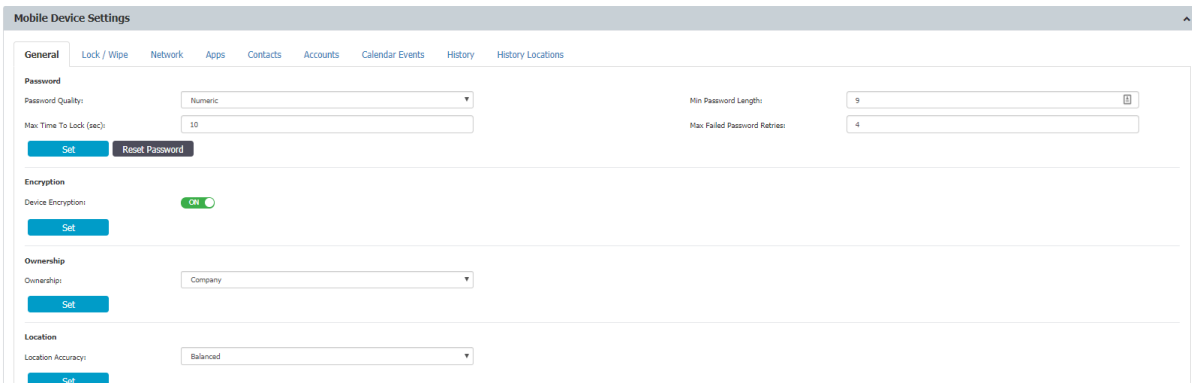
The following Settings can be applied for the password / passcode settings for an Android device:

- **Password Quality** – The following settings can be chosen from:
 - **No requirement**
 - **Any**
 - **Numeric**
 - **Alphanumeric**
 - **Complex**
- **Min Password Length** – Minimum number of digits
- **Max Time to Lock (seconds)** – If Android device is not used the device will lock (request password to access again) after set number of seconds.
- **Max Failed Password Retries** – Means the number a user can enter a wrong password until the device will wipe all data and reset itself. In case of reset, the device is wiping its entire data and is reset to a factory default. All data on the device is erased and cannot be recovered.
- **Ask User to change password** – Checking this option will prompt the device user to change from current password to a new password.

To apply the password Policy to the device, make the selection and click “Apply”.

11.1.2. Device Password

Mobile Devices > Security Policy > Device Password



The screenshot displays the 'Mobile Device Settings' window with the 'General' tab selected. The 'Password' section is active, showing the following configuration:

- Password Quality:** Numeric
- Max Time To Lock (sec):** 10
- Min Password Length:** 9
- Max Failed Password Retries:** 4

Buttons for 'Set' and 'Reset Password' are visible below the password settings. The 'Encryption' section shows 'Device Encryption' is turned ON. The 'Ownership' section is set to 'Company', and the 'Location' section is set to 'Balanced'.

The Administrator can set a password and send it to the Android device. This is helpful in case a user has forgotten the device password or the device screen does not accept user input and the device password has to be changed or set to zero.

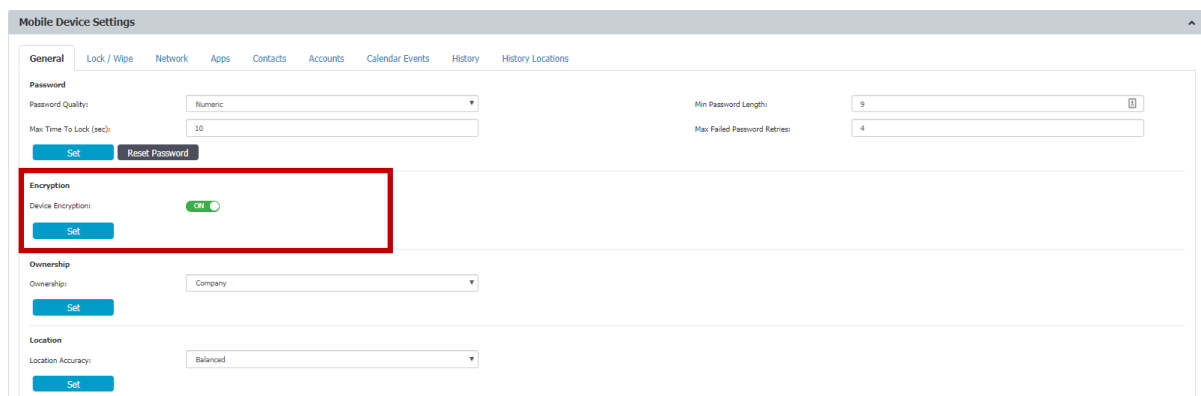
To apply the device password to the device, make the selection and click "Set".

11.1.3. Android Device Hardware Encryption

When the password/passcode for an Android device which has Android Version 4+ is set the Android device is automatically using its built in hardware encryption in order to protect data on the device in case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection. Earlier Android devices with older versions of Android do not offer this functionality.

11.2. Request Storage Encryption

The administrator can request the Android device's owner/user to encrypt the storage of the device by pressing "Enable Encryption".



A message on the device will request the encryption. The request must be accepted, then the encryption type must be chosen (quick or normal). The encryption can be started only if the following requirements are met:

- Complex password to be set
- At least 80% battery remaining on the device

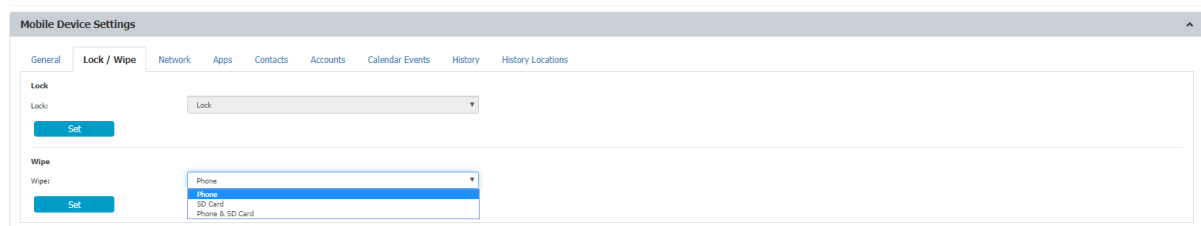
After these steps the encryption will start and the device cannot be used until the encryption is finished.

Note

The data on the SD Cards will not be encrypted!

11.3. Remote Android Lock of Device

Mobile Devices > Lock / Wipe > Lock Device



The Android device can be remotely locked. Clicking “Lock” will remotely lock the device screen and require a password entry to unlock the screen.

The device can be locked with the current password being kept “Lock Device Screen (Keep Current Password)” or alternatively be locked with a random password if selected “Strong Password Lock (Set Random Password).”

The remote lock of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote locking of the device will still work as long as the lock command can reach the device.

The Android device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device, click “Wipe” and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

Additionally, to wiping the data on the actual device the option to “Include SD Card” can be selected to also wipe the data on an SD Card in the device.

After a remote wipe the device is unmanaged. No more connection between the Android device and Endpoint Protector is possible after the remote wipe.

The remote wipe of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote wipe of the device will still work as long as the wipe command can reach the device.

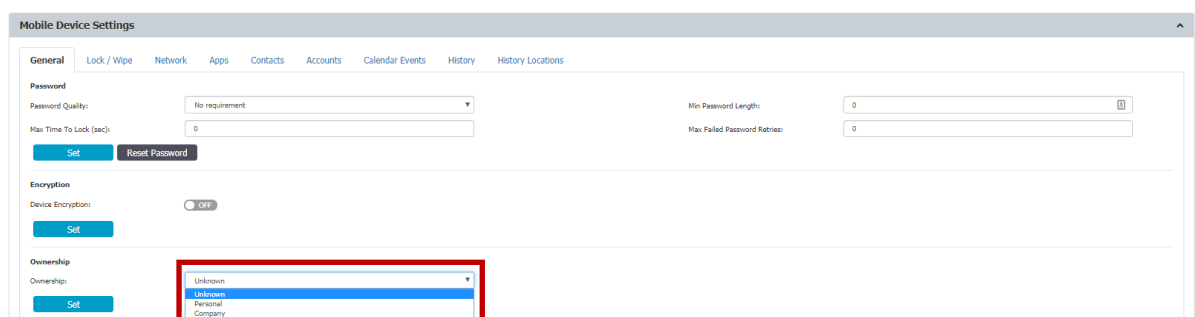
⚠ Note

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort.

The SD Card in an Android device can be remotely wiped using this feature. To wipe the SD Card click “Wipe SD-Card”.

11.4. Device Ownership

Mobile Devices > Device Settings > Device Ownership

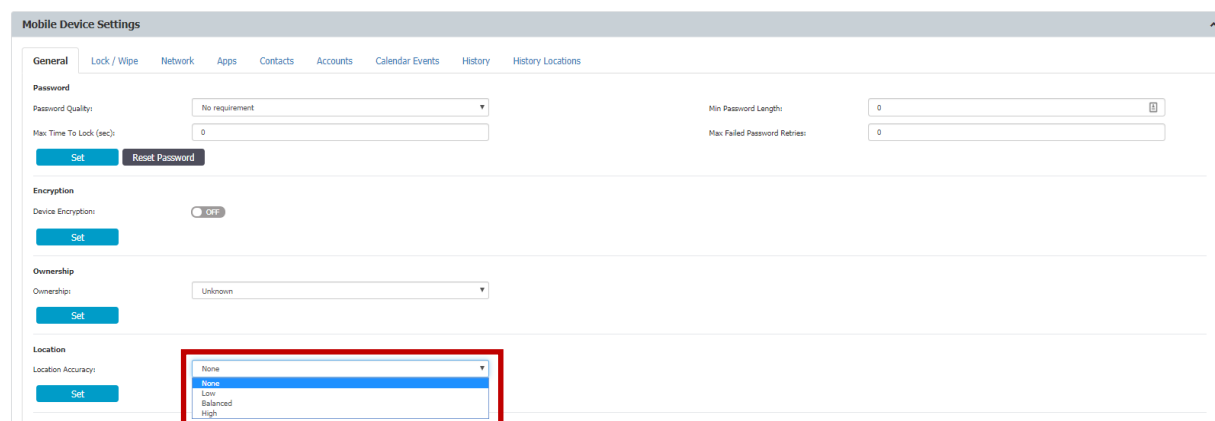


The screenshot shows the 'Mobile Device Settings' window with the 'General' tab selected. Under the 'Ownership' section, the 'Ownership' dropdown menu is open, showing three options: 'Unknown', 'Personal', and 'Company'. The 'Company' option is highlighted in blue. A red box is drawn around the dropdown menu.

The option “Device Ownership” can be set to who is the rightful owner of a device. Set it to “Company” if the company has purchased the device for the user or to “Personal” if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is set to “Unknown”.

11.5. Android Device Location Settings

Mobile Devices > Device Settings > Device Location Settings



The screenshot shows the 'Mobile Device Settings' window with the 'General' tab selected. Under the 'Location' section, the 'Location Accuracy' dropdown menu is open, showing four options: 'None', 'Low', 'Balanced', and 'High'. The 'None' option is highlighted in blue. A red box is drawn around the dropdown menu.

These settings impact the accuracy of the location data used to locate an Android device.

11.5.1. Location Accuracy Fine on Android

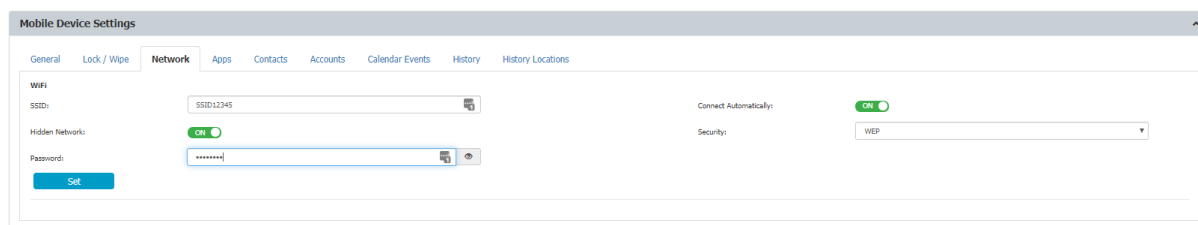
The setting “Location Accuracy Fine” unchecked relies on data from WiFi or triangulation. Checked “Location Accuracy Fine” will rely on GPS data.

11.5.2. Location Cost Allowed on Android

The setting “Location Cost Allowed” will send location data even if device is outside of the regular network.

11.6. Manage Wi-fi

This feature will enable or disable the Wi-Fi on the Android device.

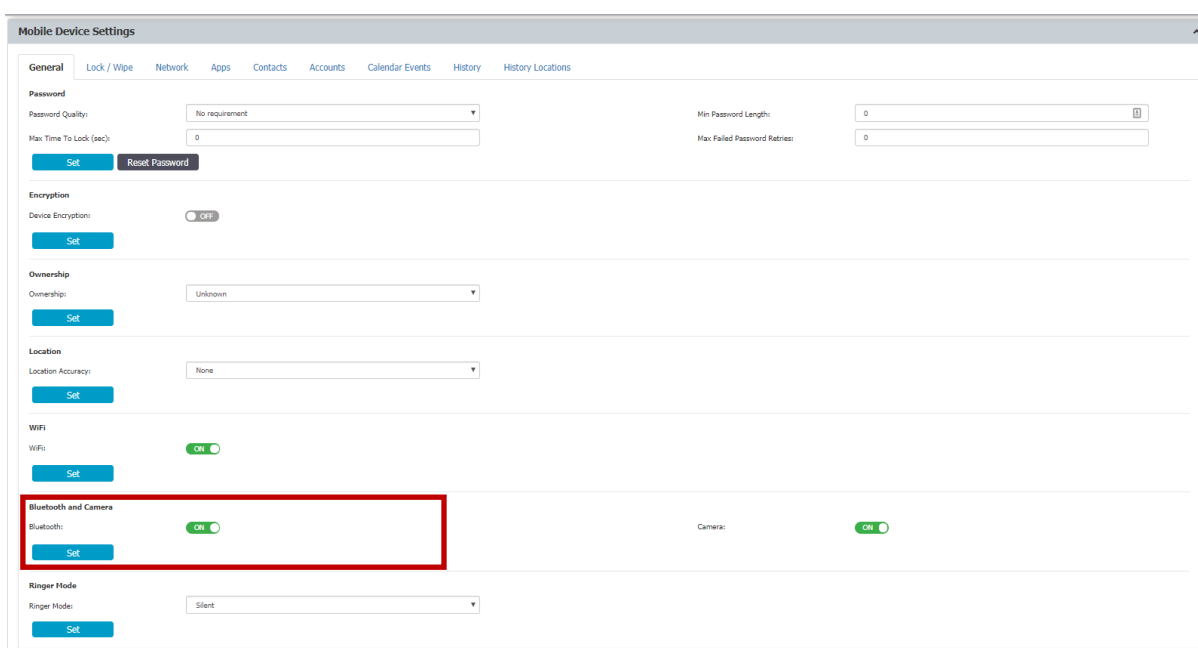


The screenshot shows the 'Mobile Device Settings' interface with the 'Network' tab selected. The 'WiFi' section is visible, containing fields for SSID (SSID12345), Hidden Network (ON), Password (masked), Connect Automatically (ON), and Security (WEP). A 'Set' button is located below the password field.

Note! Make sure that you have a valid internet connection (other than Wi-Fi) otherwise the communication between the EPP Server and the Android devices will not be possible!

11.7. Manage Bluetooth Camera

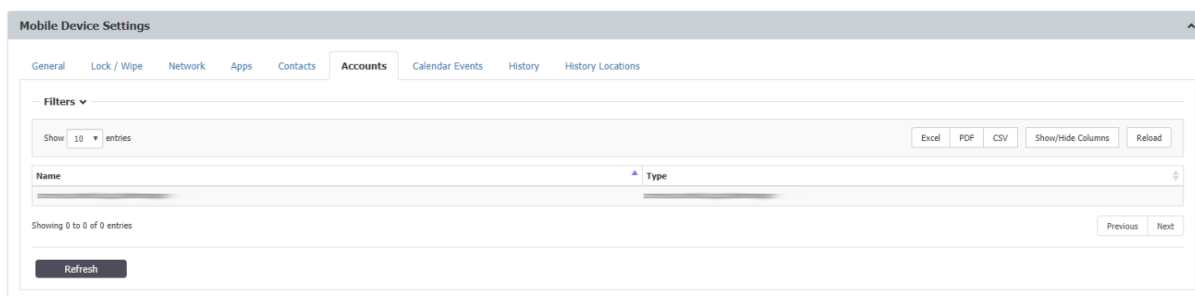
This feature will enable or disable the Bluetooth and camera on the Android device.



The screenshot shows the 'Mobile Device Settings' interface with the 'General' tab selected. The 'Bluetooth and Camera' section is highlighted with a red box, showing both Bluetooth and Camera toggles set to 'ON'. Other sections visible include Password, Encryption, Ownership, Location, and Ringer Mode.

11.8. Refresh Google Accounts for Android

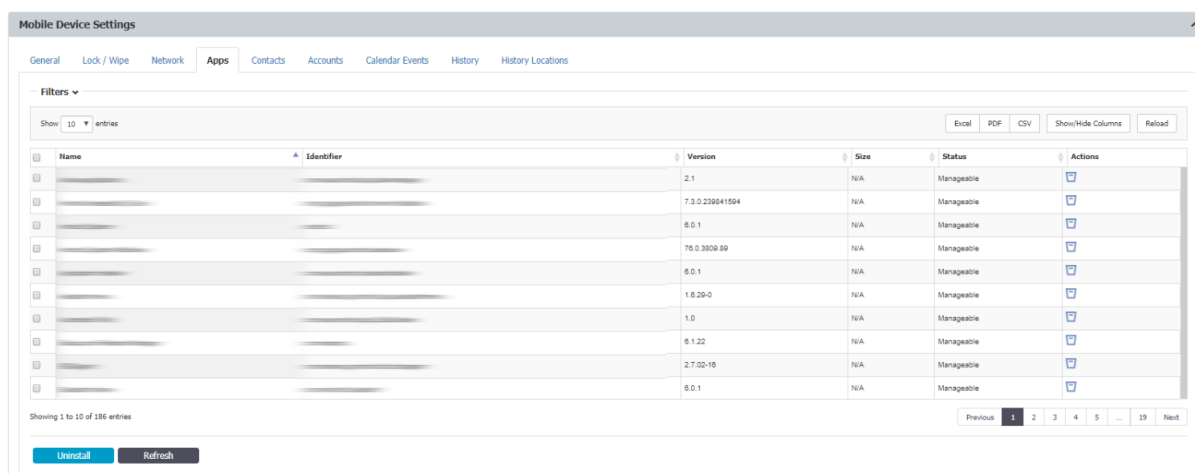
Mobile Devices > Manage Device > Accounts



Clicking “Refresh” will get the list of accounts registered on the Android device.

11.9. Refresh App List for Android

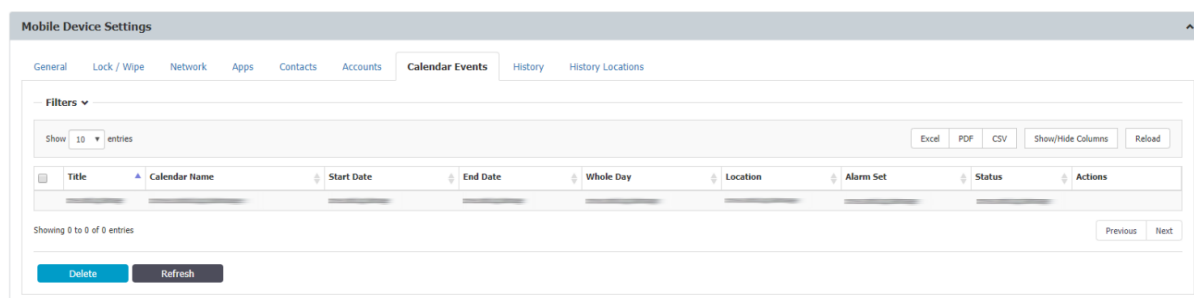
Mobile Devices > Manage Device > Apps > Refresh



This function by clicking “Refresh” will ask the Android device for a list of all the apps installed on the Android device. The list of all installed Apps is shown in Endpoint Protector MDM at Mobile Devices > Apps

11.10. Manage Calendar Events

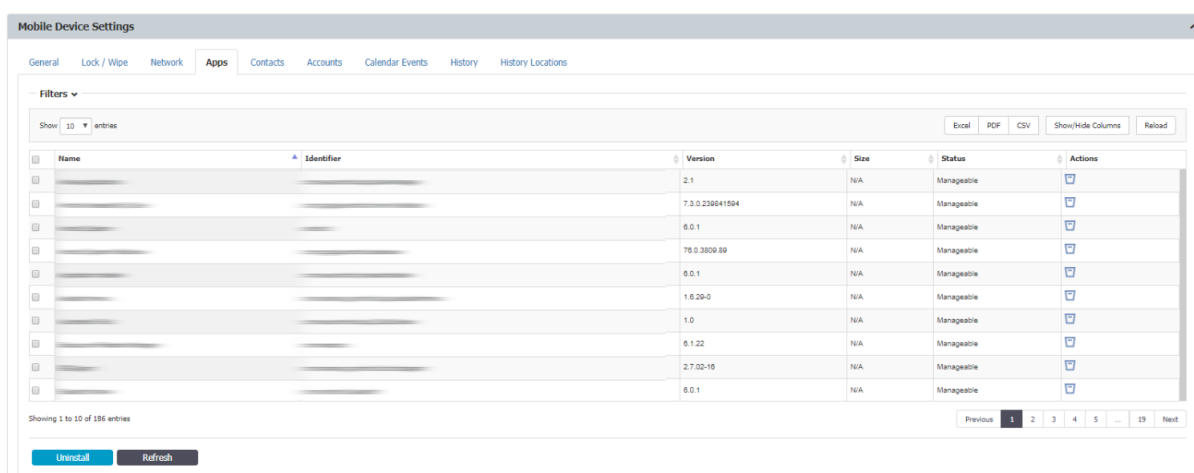
Through this feature it is possible to manage Calendar Events for Android devices. The list of the existing events can be updated by pushing the “Refresh” button.



11.11. Installed Apps on Android

Mobile Devices > Installed Apps

The List of Apps installed on the Android device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the Android device and updated through the option “Get App List” as described in chapter 11.9.



In future versions of Endpoint Protector MDM more features for managing apps on iOS Devices will be introduced.

11.11.1. Removing Installed Apps on Android

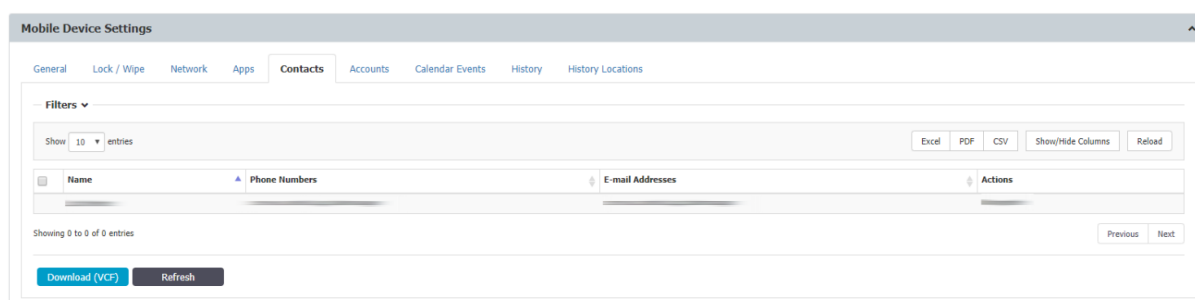
The Endpoint Protector Administrator can send an action to the Android device and ask the device to remove the app from the device. By clicking the [Remove] „Remove App” button the request is sent to the device. The Android device will now show the user that the device is supposed to be removed. The user can oppose removal and simply deny this. In this case the Administrator should send another request for removal. Due to the Androids Operating System, in the current scenario the App cannot be forcefully uninstalled.

11.12. Get Contacts on Android

Mobile Devices > Contacts

The tab “Contacts” lists all contacts that are saved in the address book of an Android device.

To retrieve the list of contacts on the device the Endpoint Protector Administrator can request the list by clicking “Refresh” under the option Mobile Devices > Manage Devices > Refresh.

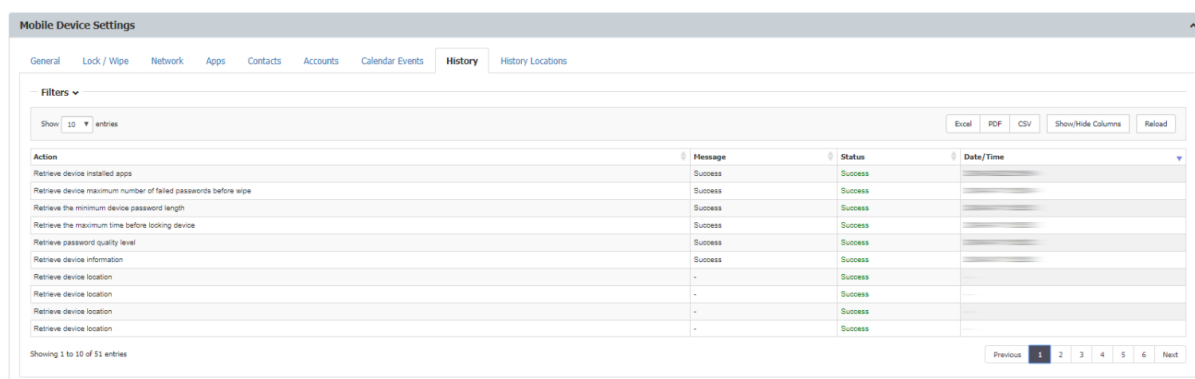


Also the download of contacts in a .vcf file format is possible by using the selection boxes and the „Download (VCF)” button.

11.13. History of Android Device Actions

Mobile Devices > History

In the “History” tab a record of actions sent to an Android device are saved and the corresponding results is shown as well. The result can be executed, error, failed or pending.



11.14. Manage Wi-Fi, Manage Mail, Profiles on Android

Mobile Devices > Manage Wi-Fi

Mobile Devices > Manage Mail

Mobile Devices > Profiles

The tabs “Manage Wi-Fi”, “Manage Mail” and “Profiles” have no functionality associated with them for Android and show “No Results”. This function is currently only supported for iOS devices.

12. Mobile Application Management (MAM) for iOS

The Mobile Application Management (MAM) feature in Endpoint Protector for iOS gives the Endpoint Protector Administrator the power to push Apps from the App store on managed iOS devices. The feature in the current version supports paid and free apps listed on iTunes App Store. (The feature supports paid and free apps listed on iTunes App Store and enterprise apps that are developed "in-house") Mobile Apps can be managed under the following option Mobile Device Management > iOS App Management.

The screenshot displays the Endpoint Protector web interface. The left sidebar contains a navigation menu with categories like Dashboard, Device Control, and Mobile Device Management. The main content area is titled "Mobile Device Management - iOS App Management". It features a search bar for the iTunes App Store and a table of search results. The table lists one app: "EPP MDM" by ColSya, version 1.2, which is free and categorized as a utility. Below the search results, there is a "Manage iOS Apps" section with a table showing the same app and a "Push iOS Apps" button.

Select	Icon	Title	Vendor	Version	Description	Price	Category	iPhone	iPad	Actions
<input type="checkbox"/>		EPP MDM	ColSya	1.2	Endpoint Protector Mobile Device Management provid...	Free	Utilities			

OS	Icon	Title	Vendor	Version	Description	Price	Codes	Category	Flags	iPhone	iPad	Actions
iOS		EPP MDM	ColSya	1.2	Endpoint Protector Mobile Device Management provides complete iOS ente...	Free		Utilities		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

12.1. Adding Apps to your Managed Apps Catalog

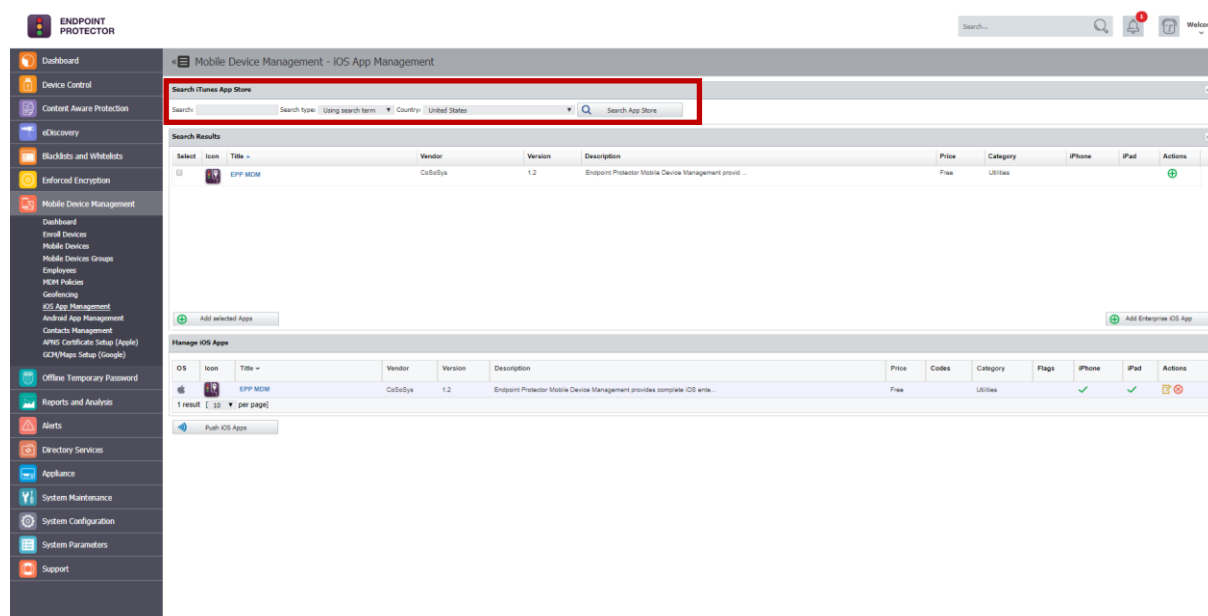
To add Apps search for the App in the iTunes App Store directly in the Endpoint Protector interface.

12.1.1. Searching for Apps



Searching for Apps is possible by entering the name of the App or by directly entering the App ID of an App (e.g. the App ID for the EPP MDM iOS App is id570954584). The App ID is stated in the URL of an app when viewing the app details in a web browser



(e.g. <https://itunes.apple.com/us/app/epp-mdm/id570954584>).

For either type of search selects “Using search term” or “Using iTunes App ID”.



The screenshot displays the Endpoint Protector web interface. The left sidebar contains navigation options such as Dashboard, Device Control, Content Aware Protection, eDiscovery, Blacklists and Whitelists, Enforced Encryption, and Mobile Device Management. The main content area is titled "Mobile Device Management - iOS App Management". A search bar at the top of this section is highlighted with a red box, showing the search type "Using search term" and the country "United States". Below the search bar, the "Search Results" table lists one app: "EPP MDM" by "CoSoBye", version 1.2, with a price of "Free" and category "Utilities". The table also shows columns for iPhone and iPad availability, both marked with green checkmarks. Below the search results, there is a "Manage iOS Apps" section with a table listing the same app and a "Push iOS Apps" button.

Select	Icon	Title	Vendor	Version	Description	Price	Category	iPhone	iPad	Actions
<input type="checkbox"/>		EPP MDM	CoSoBye	1.2	Endpoint Protector Mobile Device Management provides complete iOS anti...	Free	Utilities	✓	✓	

OS	Icon	Title	Vendor	Version	Description	Price	Codes	Category	Flags	iPhone	iPad	Actions
iOS		EPP MDM	CoSoBye	1.2	Endpoint Protector Mobile Device Management provides complete iOS anti...	Free		Utilities		✓	✓	

12.1.2. Adding Apps to Managed Apps Catalog

To add an App to your Managed Apps Catalog, select the App from the “Search Results” and click “Add selected Apps”.

The screenshot shows the 'Mobile Device Management - iOS App Management' interface. The 'Search Results' table contains the following data:

Select	Icon	Title	Vendor	Version	Description	Price	Category	iPhone	iPad	Actions
<input type="checkbox"/>		EPP MDM	CoSulys	1.2	Endpoint Protector Mobile Device Management provid...	Free	Utilities			

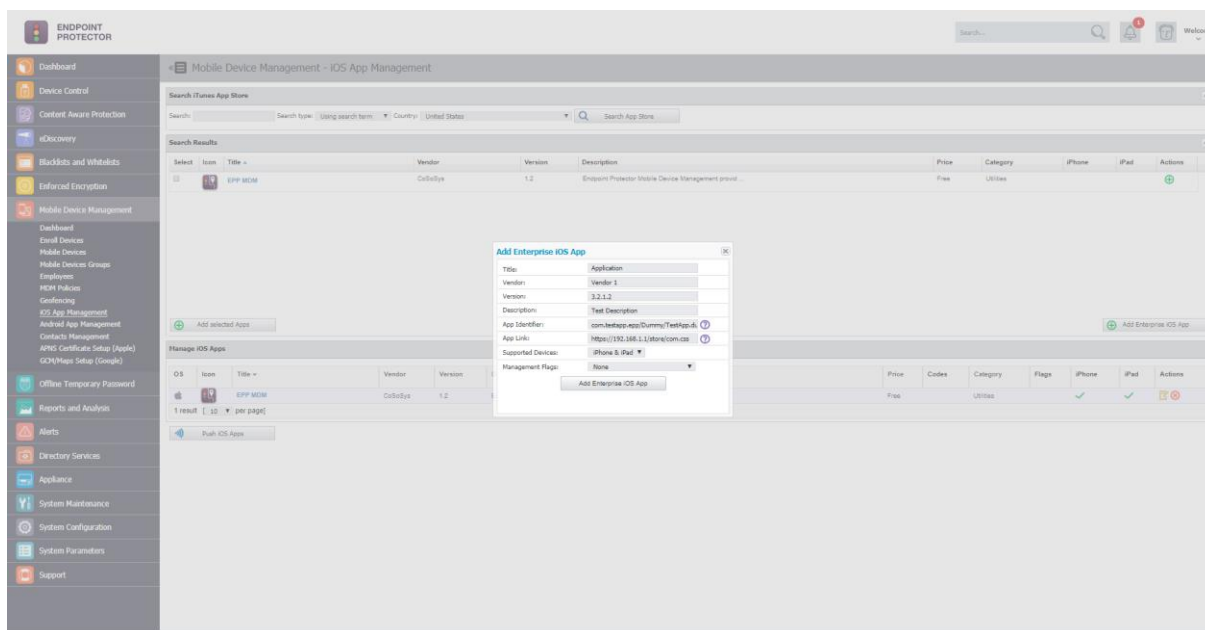
Below the table, the 'Add selected Apps' button is highlighted with a red box.

12.1.3. Adding „Enterprise Apps“ to Managed Apps Catalog

You can add applications developed „in-house“ by clicking on the „Add Enterprise App“ button.

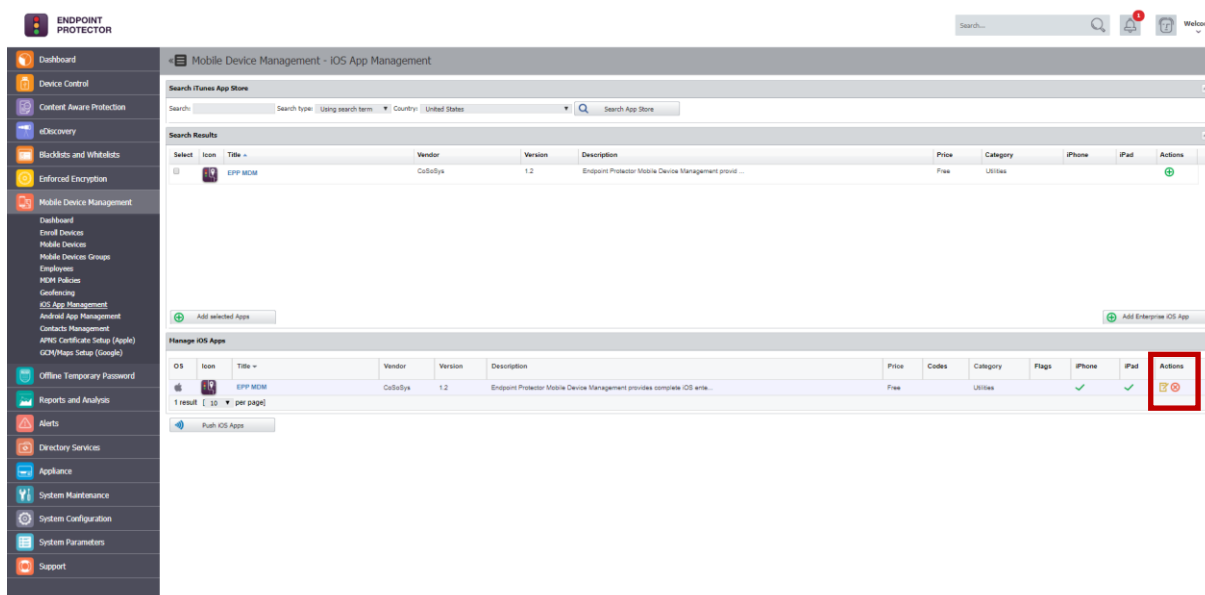
The screenshot shows the 'Mobile Device Management - iOS App Management' interface. The 'Add Enterprise iOS App' button is highlighted with a red box.

You will have to enter the required details in the pop-up window.





12.2. Editing App Management Options

Managed Apps options can be modified by selecting "Edit App".



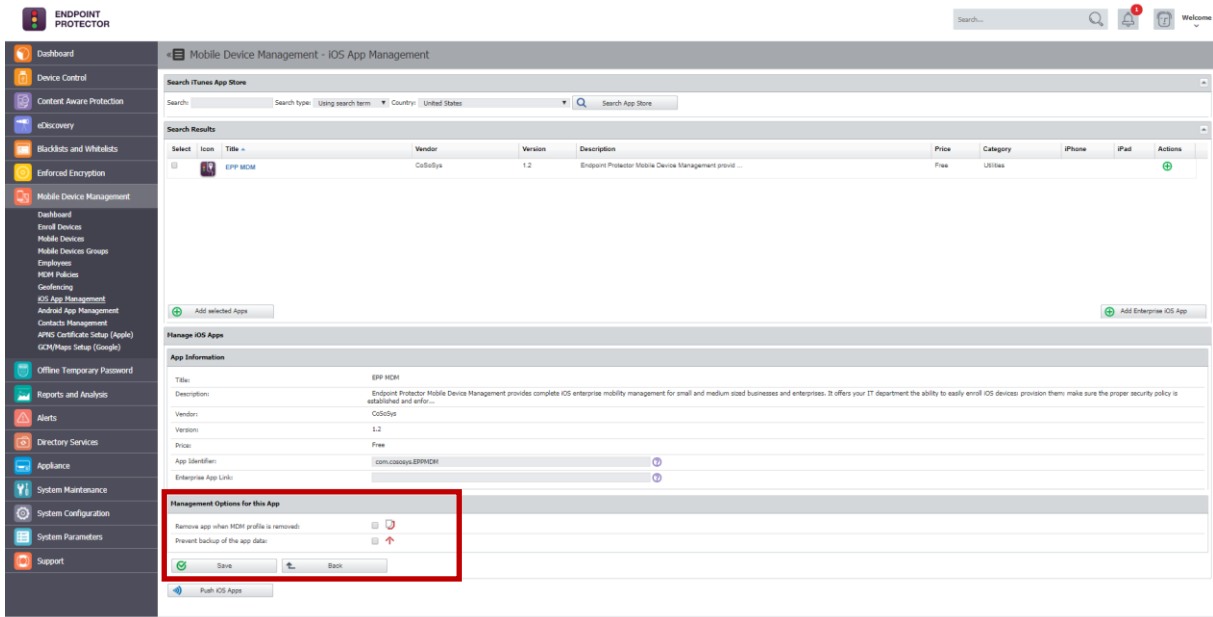
Management Options for this App

Remove app when MDM profile is removed: 

Prevent backup of the app data: 

The options for managed Apps are:

- Remove app when MDM profile is removed**
 if this management flag is set the managed App and all its associated data/content with it, will be removed if the iOS device becomes unmanaged, either if the Endpoint Protector administrator unmanages the device or if the device user is unmanaging the device by removing the device enrollment profile.
- Prevent backup of the app data**
 if this management flag is set the managed Apps associated data/content will not be backed up in case the device is synced or backed up with iTunes.

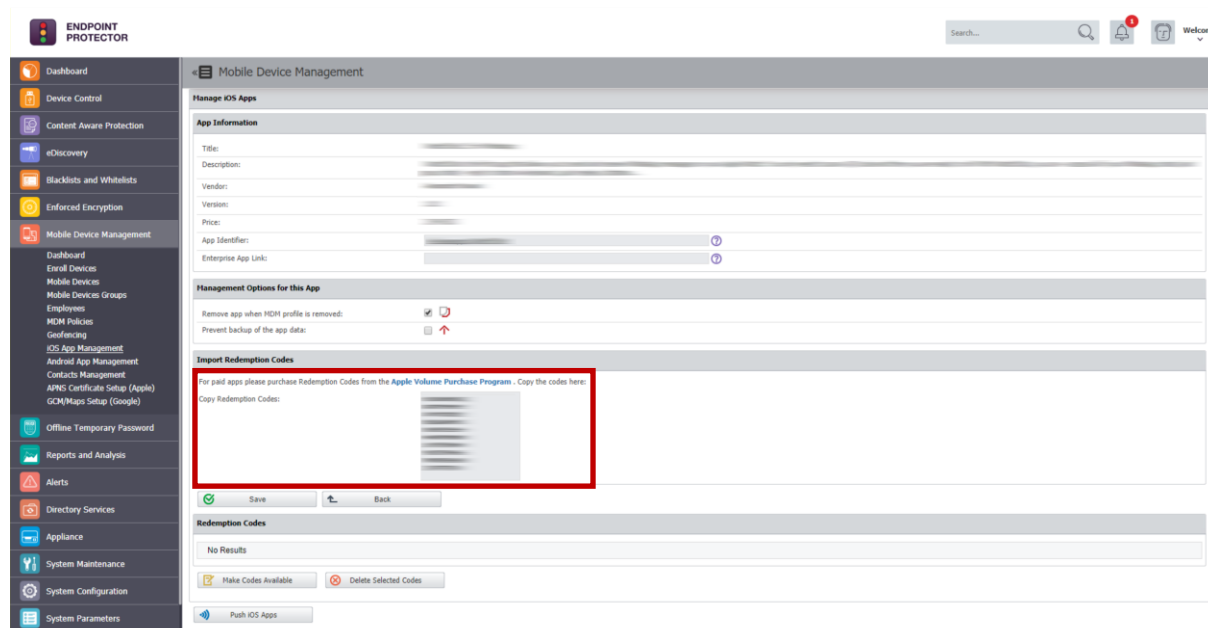


12.3. Managed Paid Apps

Paid Apps require purchasing license keys through the Apple Volume Purchase Program. The licenses (which Apple calls Redemption Codes) can be purchased here: <https://vpp.itunes.apple.com>.

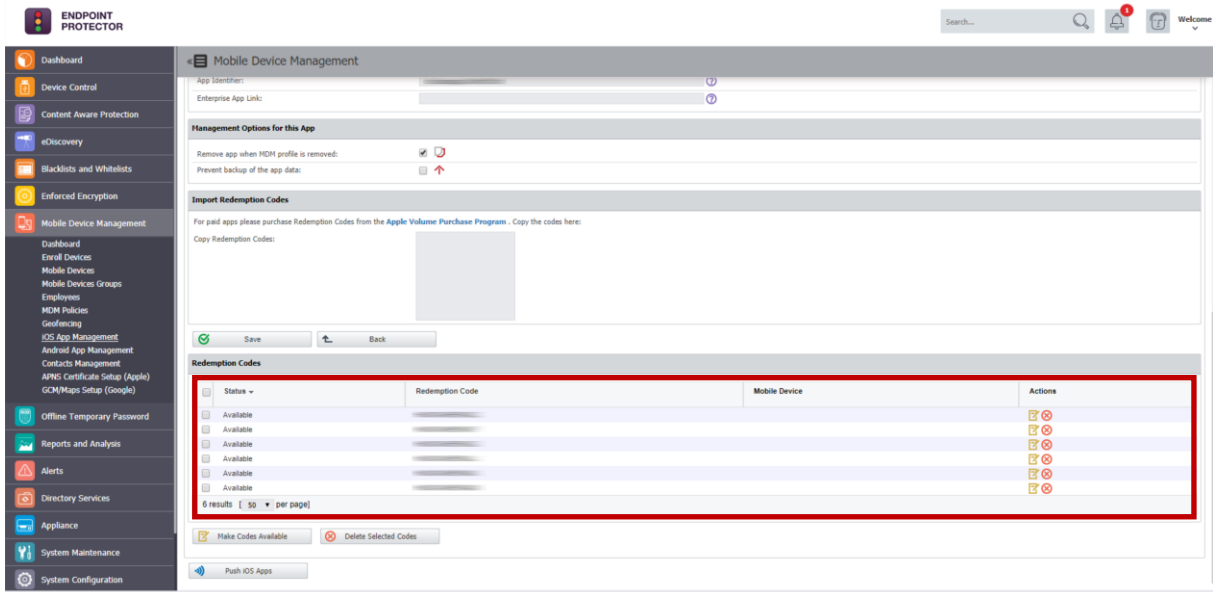
This option is available in the Endpoint Protector interface only for paid apps when selecting “Edit App” under the point “Import Redemption Codes”.

After redemption codes have been purchased from Apple they need to be introduced through copy/pasting the redemption codes into the Endpoint Protector interface under the option “Edit App” > Import Redemption Codes.



The screenshot displays the Endpoint Protector web interface for Mobile Device Management. The left sidebar contains a navigation menu with options like Dashboard, Device Control, Content Aware Protection, eDiscovery, Blacklists and Whitelists, Enforced Encryption, and Mobile Device Management. The main content area is titled 'Manage iOS Apps' and shows details for a selected app, including App Information (Title, Description, Vendor, Version, Price, App Identifier, Enterprise App Link) and Management Options (Remove app when MDM profile is removed, Prevent backup of the app data). The 'Import Redemption Codes' section is highlighted with a red box and contains the instruction: 'For paid apps please purchase Redemption Codes from the Apple Volume Purchase Program. Copy the codes here:'. Below this is a text area for 'Copy Redemption Codes' and buttons for 'Save' and 'Back'. The 'Redemption Codes' section below shows 'No Results' and buttons for 'Make Codes Available' and 'Delete Selected Codes'.

After adding the redemption codes click “Save”. The saved redemption codes will be listed under “Edit App” > Redemption Codes.



All redemption codes show their status either as available or used in case they have been used, meaning a code was used when a paid app was pushed to a device which did not already have this paid app installed.

Additionally the number of total and still available (not yet consumed) redemption codes is shown in the column “Codes” in the list of “Managed iOS Apps”. In the example below 10/10 meaning ten of ten codes are available.

OS	Icon	Title	Vendor	Version	Description	Price	Codes	Category	Flags	iPhone	iPad	Actions
		WhatsApp Messenger	WhatsApp Inc.	2.8.7	WhatsApp Messenger is a cross-platform smartphone messenger currently ...	0.99 USD	10/10	Social Networking				
		iBooks	Apple Inc.	3.1	iBooks is an amazing way to download and read books. iBooks includes t...	Free		Book				
		EPP MDM	CoSoSys	1.0.0.6	Endpoint Protector Mobile Device Management provides complete iOS ente...	Free		Utilities				
		Adobe Reader	Adobe Systems, Inc.	10.5.2	Adobe® Reader® is the free, trusted leader for reliably viewing and ...	Free		Business				

12.4. Pushing Apps to iOS Devices

The list of Managed Apps is available when viewing the details about any managed iOS device in the tab “Apps”.

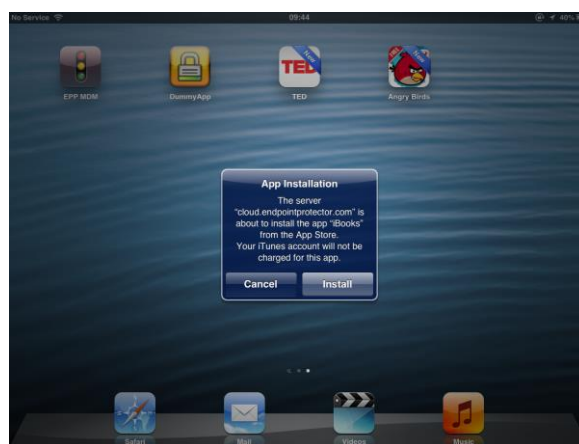
The screenshot shows the Endpoint Protector Mobile Device Management interface. The main content area is titled "Mobile Device Settings" and has tabs for "General", "Restrictions", "Lock / Wipe", "Network", "Mail", "Apps", "Profiles", "History", and "History Locations". The "Apps" tab is selected, displaying a table of installed apps. A red box highlights the trash icon in the "Actions" column for the "EPP MDM" app.

Name	Identifier	Version	Size	Status	Actions
Drive	com.microsoft.office.drive	1.3.964	25 MB	Not Manageable	-
Emoji	gnaemem.emoji	4.3	76.19 MB	Not Manageable	-
EPP MDM	com.casops.EPPMDM	1.2	13.25 MB	Manageable	🗑️
QR Code Reader	com.zeappz.frea.QRScanner	1.0.4	5.08 MB	Not Manageable	-
sensibility.io	com.casops.sensibility.io	1.0	58.84 MB	Not Manageable	-
WhatsApp	net.whatsapp.WhatsApp	2.19.100	148.4 MB	Manageable	🗑️
Word	com.microsoft.Office.Word	2.30.1	280.84 MB	Not Manageable	-
YouTube	com.google.ios.youtube	14.40.2	104.48 MB	Not Manageable	-

Only Apps that have been added to the Managed App Catalog are displayed in this tab.

To push an app to a managed device, click the 🗑️ icon. A message will show that the app has been pushed to the device.

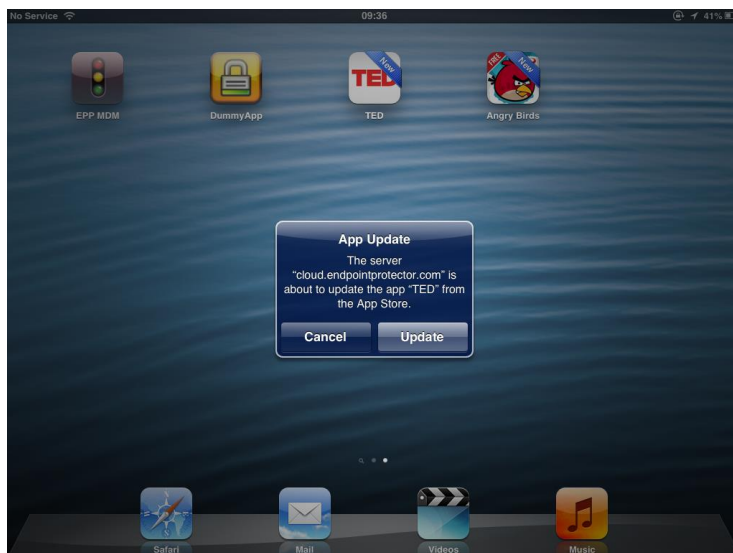
After the app has been pushed to the device the user is prompted to install the app and to provide the iTunes account password associated with the device.



Apps can also be pushed from MDM policies “Manage Apps” tab.

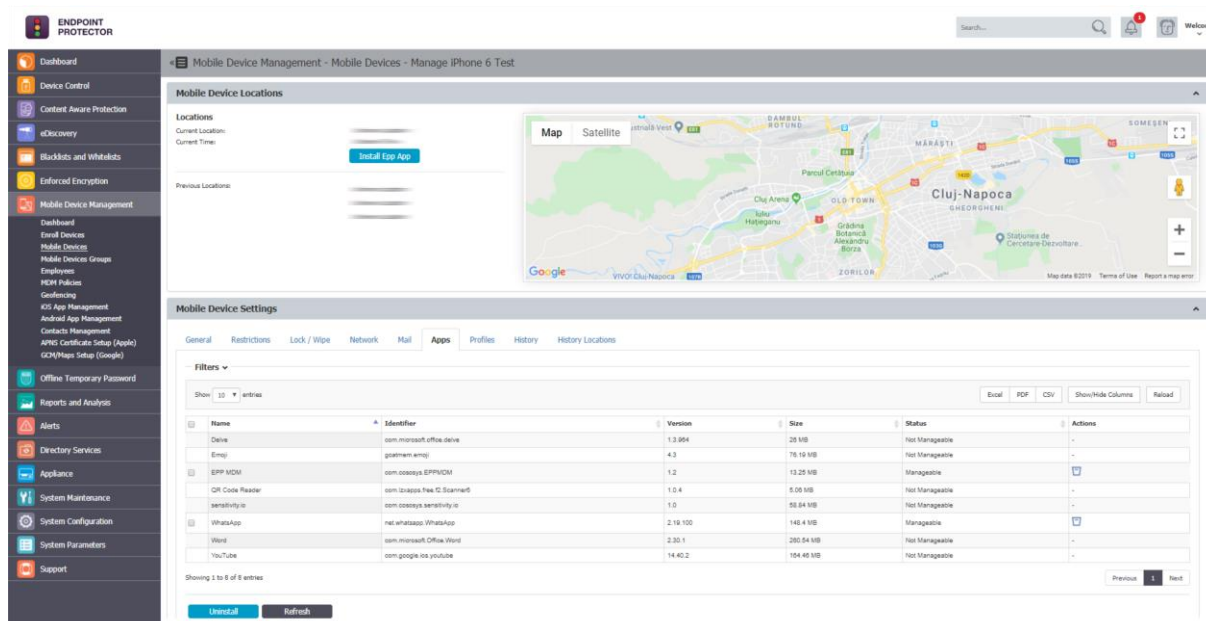
12.4.1. Update Managed Apps / Changing Settings


In case a newer version of an app is available you can update it using the same steps as when pushing a new app to a managed device. In case an update is pushed the user will be prompted to update the app. In case of paid apps, no new redemption code is consumed during this process.



12.5. Removing Managed Apps from iOS Devices

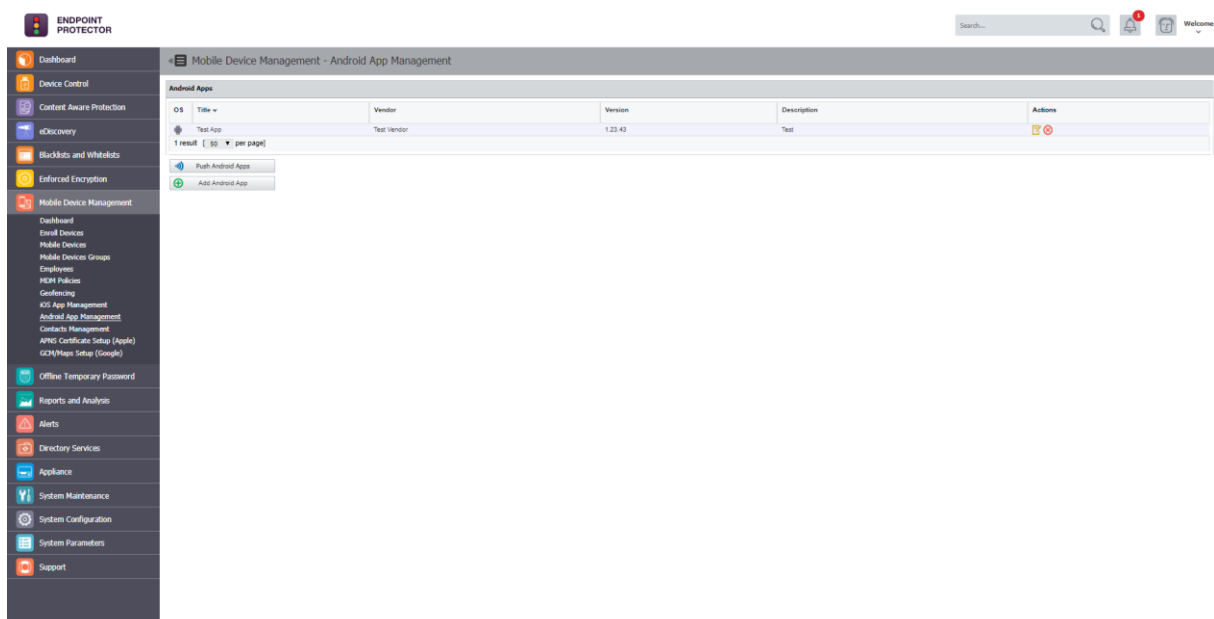
All installed Apps on a managed iOS device are displayed in the tab “Installed Apps”.



To remove an app, click the  icon and the app will be deleted from the managed iOS device. When a managed app is removed on the device the device user is not asked to confirm the removal of the app.

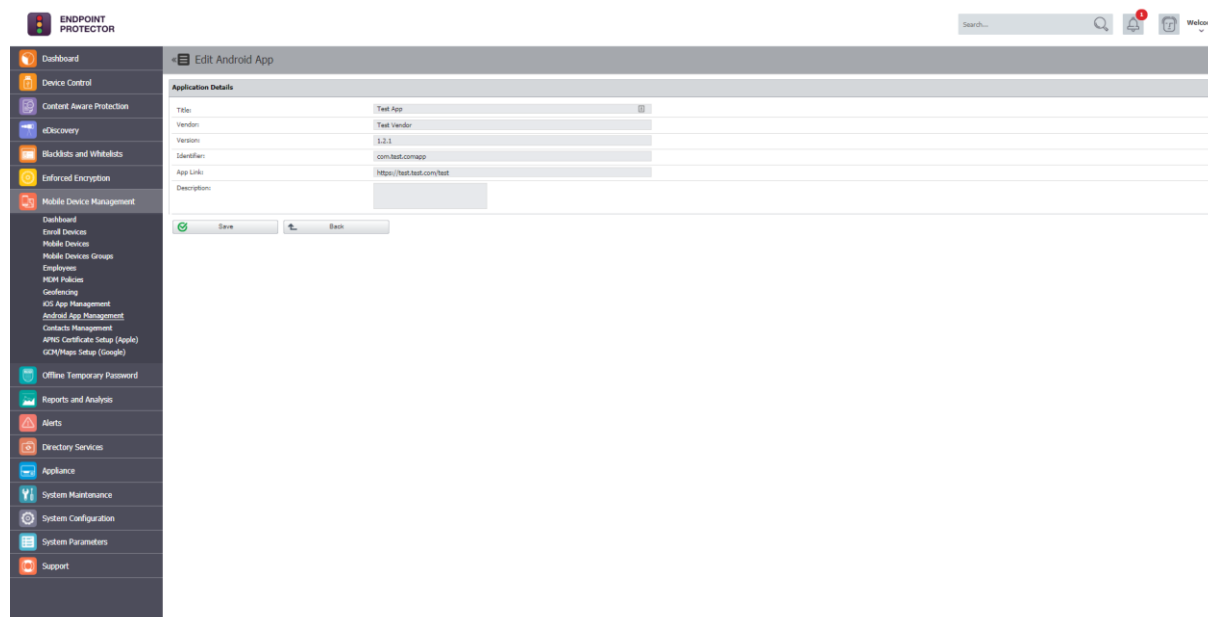
13. Android App Management

The Mobile Application Management (MAM) feature in Endpoint Protector for Android gives the Endpoint Protector Administrator the power to push Apps on managed Android devices. The feature in the current version supports “in-house” apps. Mobile Apps can be managed under the following option Mobile Device Management > Android App Management.



13.1 Adding Apps to your Managed Apps Catalog

To add Apps in the Catalog, push the “Add Android App” button, and complete the required fields. The administrator must make the application available on the internet (if it isn’t already), then the corresponding link must be entered in the “App Link” field.



13.1. Editing App Management Options

Managed Apps can be modified by selecting “Edit App” or they can be deleted by pressing the “Delete” button.

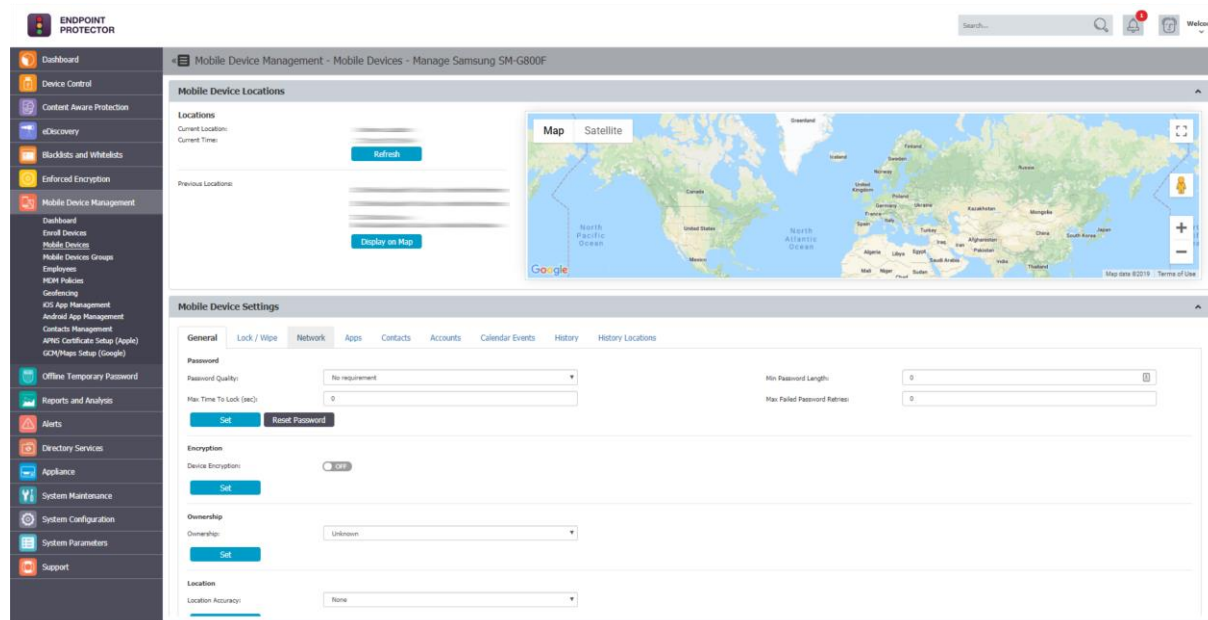
Android Apps					
OS	Title	Vendor	Version	Description	Actions
	CoSoSys Notepad Demo	CoSoSys	1.0		

1 result [50 per page]


Add Android App

13.2. Pushing Apps to Android Devices

The list of Managed Apps is available when viewing the details about any managed Android device in the “Apps” tab.



Only Apps that have been added to the “Android App Management” tab are displayed.

To push an app to a managed device, click the  icon. A message will show that the app has been pushed to the device. Multiple applications can be sent by pressing the “Push all selected apps” button.

Apps can also be pushed from Android policies’ “Manage Apps” tab.


13.3. Removing Managed Apps from Android Devices

All installed Apps on an Android device are displayed in the “Installed Apps” tab.

The screenshot displays the Endpoint Protector Mobile Device Management interface for a Samsung SM-G900F device. The interface is divided into several sections:

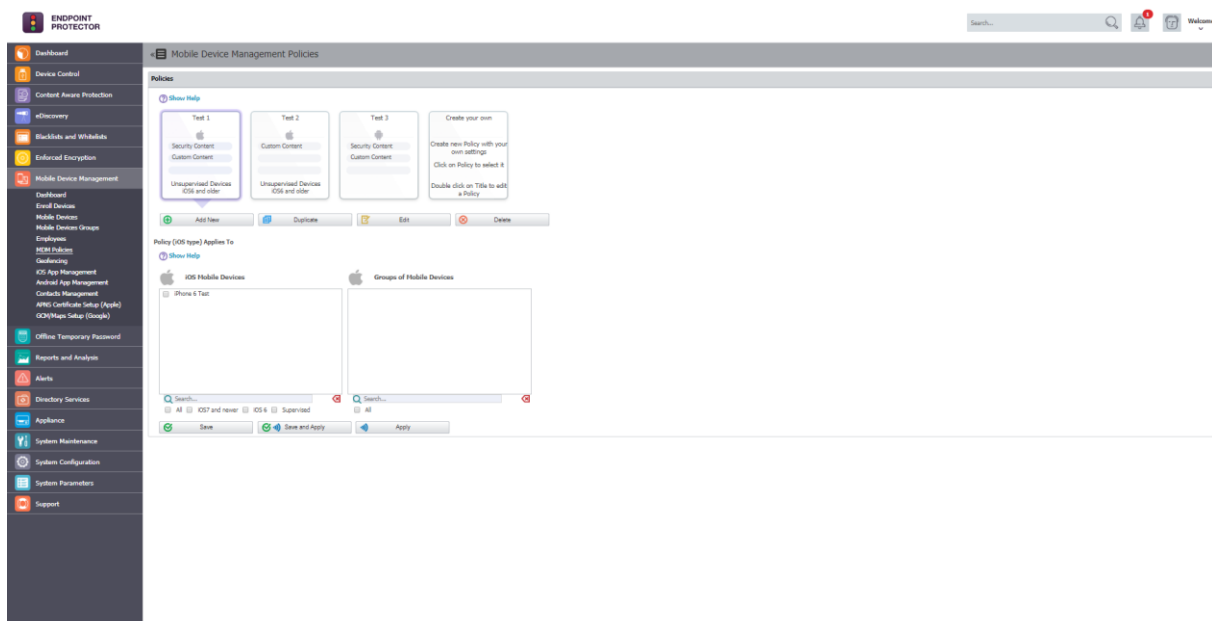
- Mobile Device Locations:** Shows current and previous locations with a map and buttons for 'Refresh' and 'Display on Map'.
- Mobile Device Settings:** A tabbed interface with 'Apps' selected. It shows a list of installed applications with columns for Name, Identifier, Version, Size, Status, and Actions.

Name	Identifier	Version	Size	Status	Actions
Active applications	com.sec.android.app.taskmanager	2.1	N/A	Managed	[Remove]
Android Accessibility Suite	com.google.android.marvin.talkback	7.0.228841084	N/A	Managed	[Remove]
Android System	android	8.0.1	N/A	Managed	[Remove]
Android System WebView	com.google.android.webview	70.0.3029.89	N/A	Managed	[Remove]
Application Installer	com.sec.android.preinstallinstaller	8.0.1	N/A	Managed	[Remove]
Assistant menu	com.samsung.android.app.assistmenu	1.0.28-0	N/A	Managed	[Remove]
Automation Test	com.sec.android.app.OtaCreate	1.0	N/A	Managed	[Remove]
Backup and Restore Manager	com.sec.android.app.OtaCreate	8.1.02	N/A	Managed	[Remove]
BBCAgent	com.samsung.android.bbc.agent	2.7.03-18	N/A	Managed	[Remove]
Bluetooth share	com.android.bluetooth	8.0.1	N/A	Managed	[Remove]

To remove an app, click the  icon and the app will be deleted from the Android device. When a managed app is removed on the device the device user is not asked to confirm the removal of the app.

14. Policy Builder for iOS, OSX or Android Devices

The Policy Builder for iOS, OS X and Android devices is located under Mobile Device Management > MDM Policies.



The advantage of using an MDM Policy is that for a large number of devices the policy can be changed simultaneously.

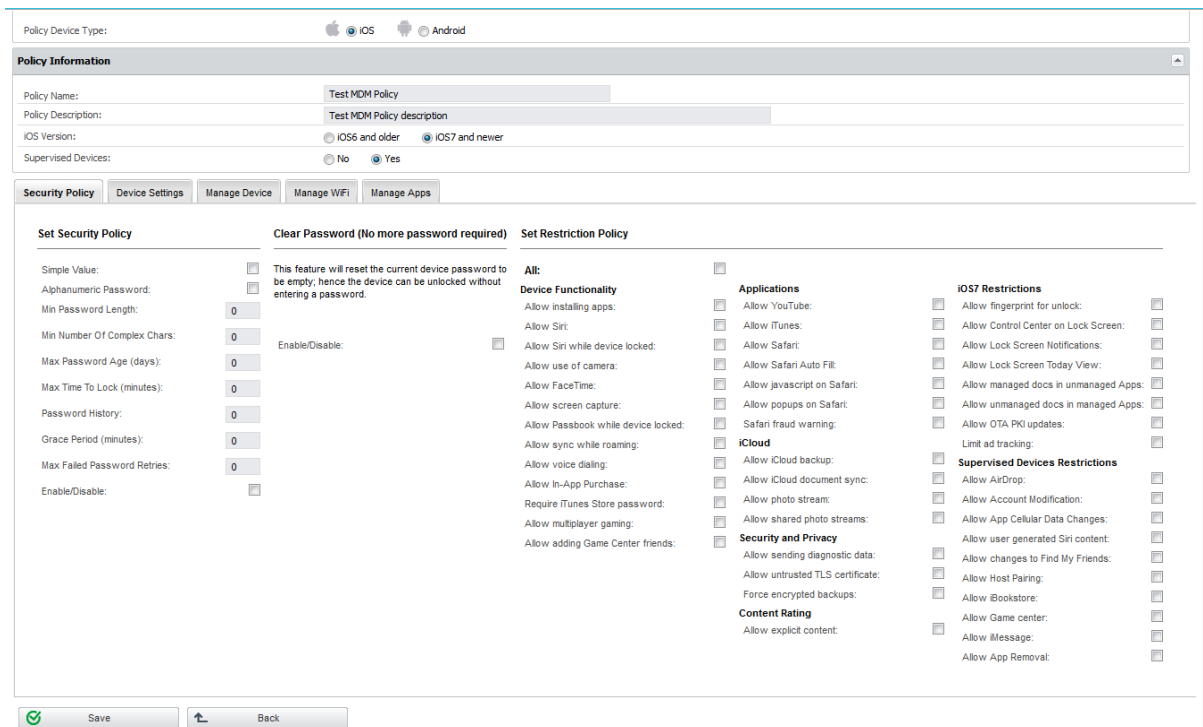
14.1. Create a Policy for iOS, OS X or Android Devices

To create a new MDM Policy, click on "Add New" and then select for what operating System the Policy should apply. Choose between iOS, OS X and Android.

Give the policy a name and a description that will help you later administering your devices easier.

Policies are based on device operating system.

Make the settings for the policy you require. For each operating system different options are available to be set in the policy.

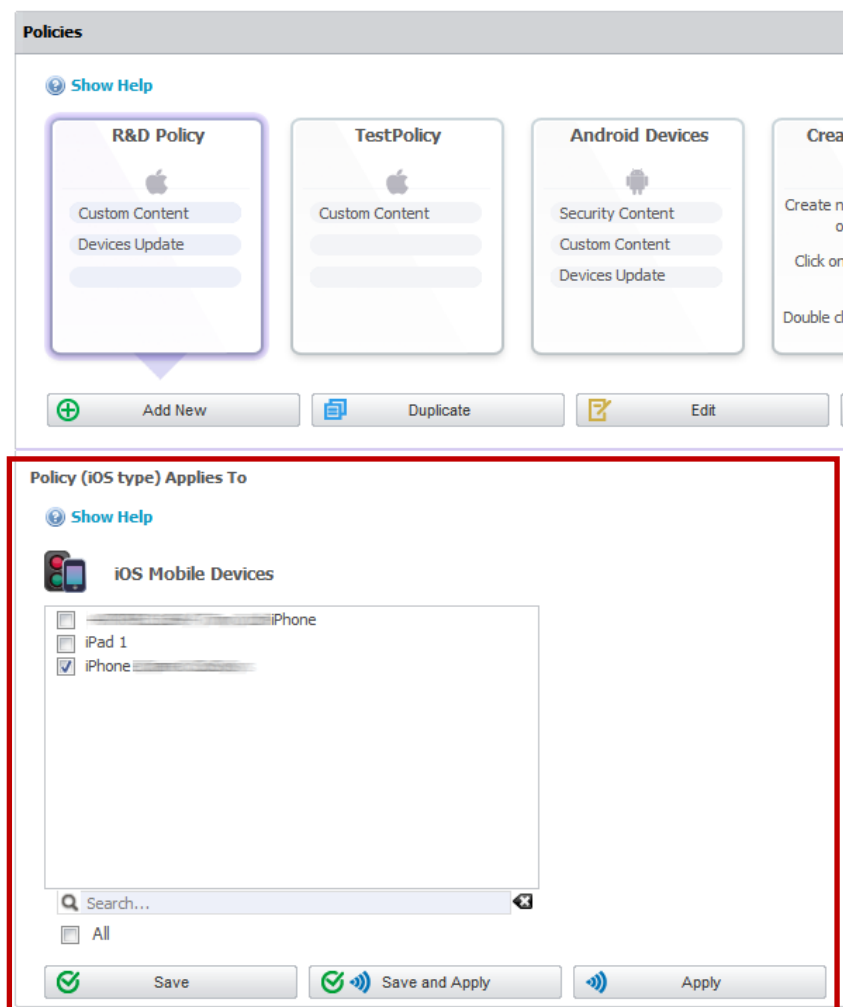


After you made the settings to the Policy click "Save".

Note
 If you select "iOS7 and newer" as your Operating System version but actually the devices Operating System is older than iOS6, the iOS7 Restrictions and Supervised Devices Restrictions won't be sent to the device.

14.2. Assigning Devices to Policy

After you created an MDM Policy you can assign devices to the policy by selecting them under “Policy (OS type) Applies To”



You can save your selection of devices by clicking “Save”. The “Save” option is not yet applying the settings from the policy to a device. Only after you click “Apply” or “Save and Apply” the policy will be applied to the devices included in the policy.

15. Unmanage a Mobile Device / Uninstall App

In case that a mobile device must no longer be remotely managed/controlled, Endpoint Protector the user (depending on rights) and Endpoint Protector Administrator can uninstall / unmanage the mobile device. The uninstall/unmanage process for Android and iOS/ OS X mobile devices is different.

15.1. iOS and OS X Device Unmanage by Administrator (over-the-air)

To unmanage an iOS or OS X device the Endpoint Protector Enrollment Profile on the iOS/ OS X device has to be removed. The Endpoint Protector Administrator can remove the profile by following the removal of profile information described in paragraph 9.14.1 (iOS)/10.11.1 (OS X). To unmanage a device it is important that the Endpoint Protector Enrollment Profile is removed. After removing of the Enrollment Profile the device status as described in chapter 8.1 Mobile Device Status will change to "MobileProfileRemoved".

15.1.1. iOS Uninstall / Unmanage by User (on Device)

To unmanage an iOS device, the Endpoint Protector Enrollment Profile on an iOS mobile device must be removed. Go to Device Settings -> General and select the Endpoint Protector Profile. The next displayed window will contain the option to "Remove" Endpoint Protector from the mobile device.

⚠ Note

Although the uninstallation can be performed by the user, the Administrator will also be notified about the removal of the Endpoint Protector Enrollment Profile.

15.1.2. OS X Uninstall / Unmanage by User (on Device)

To unmanage an OS X device, the Endpoint Protector Enrollment Profile on an OS X mobile device must be removed. Go to System Preferences ->Profiles and select the Endpoint Protector Profile and choose to remove it.

Note

Although the uninstallation can be performed by the user, the Administrator will also be notified about the removal of the Endpoint Protector Enrollment Profile.

15.2. Uninstall iOS EPP MDM app

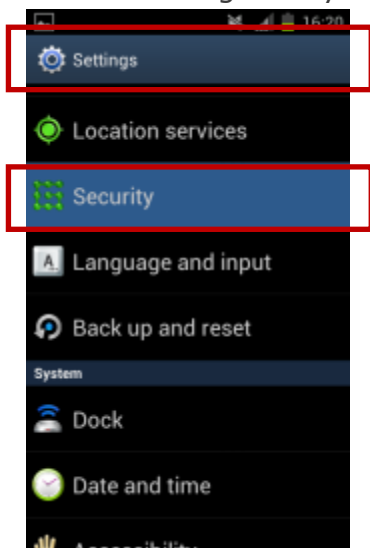
To uninstall the EPP MDM iOS app the user of the iOS device can uninstall it by pushing the EPP MDM app icon for two seconds and then deleting the app by clicking (x).

15.3. Android EPP Client App Uninstall / Unmanage Android Device

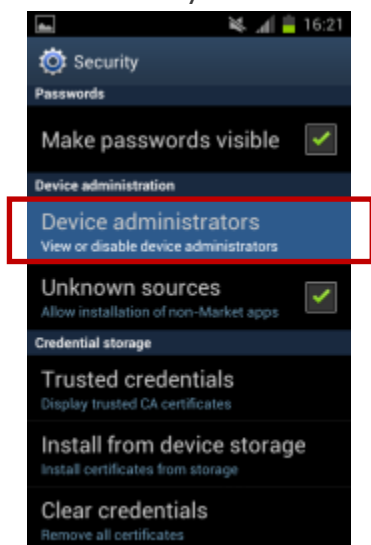
To uninstall EPP Client App on an Android Mobile Device, the user needs to disable the Device Administrator role from Device Settings.

To uninstall the EPP Client App follow these steps:

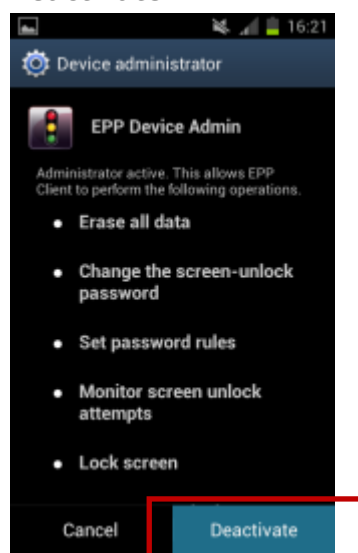
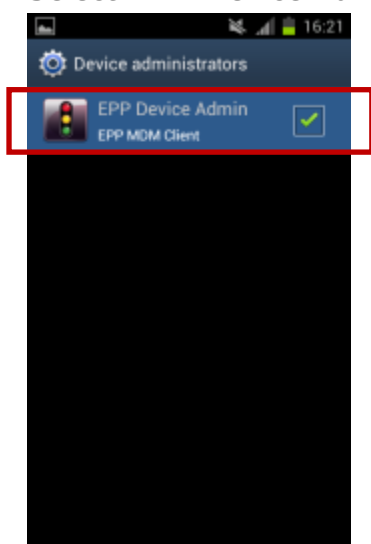
1. Go to "Settings" on your Android device and select "Security".



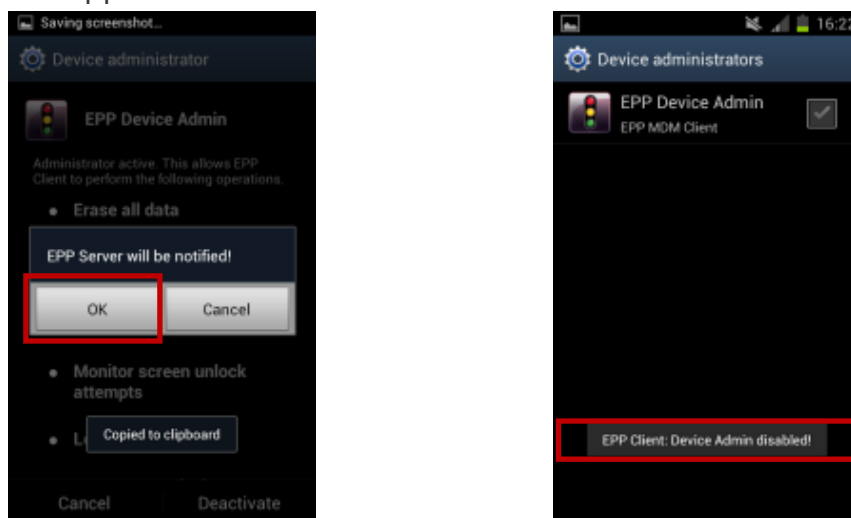
2. In "Security" select "Device administrators" and click on it.



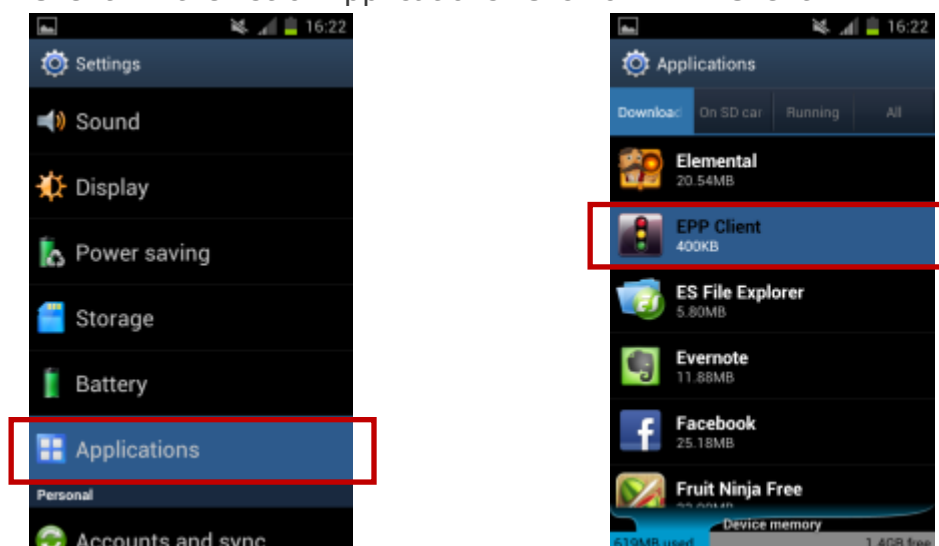
3. Select "EPP Device Admin" and click "Deactivate".



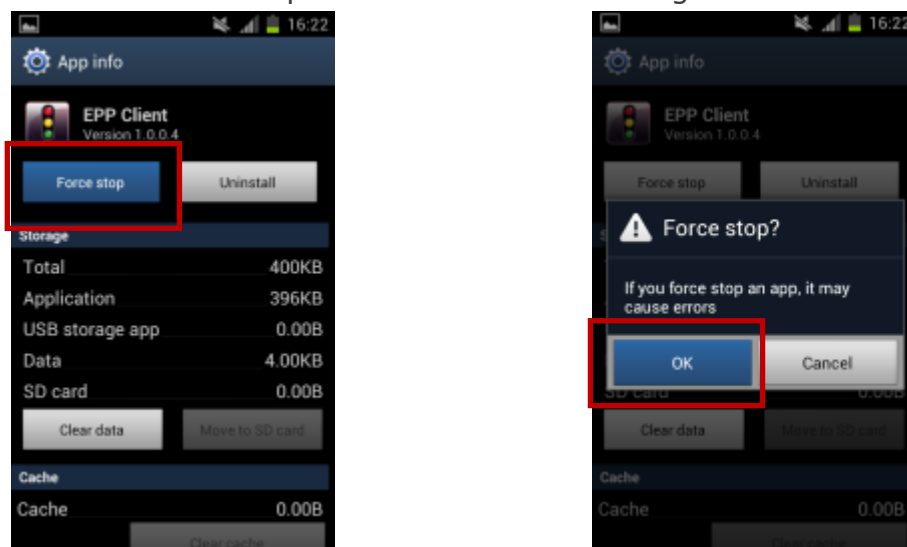
4. A pop-up will appear saying that the “EPP Server will be notified”. To continue click “OK”. A message saying “EPP Client Device Admin disabled” will appear.



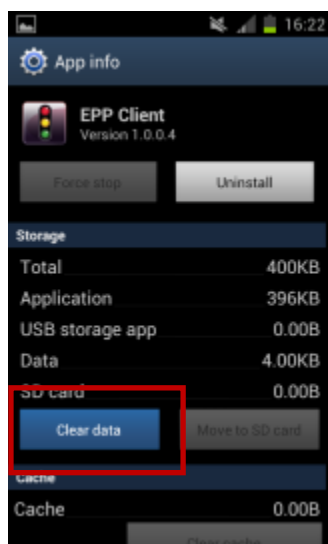
5. Now go to the “Application” menu on your Android device and locate “EPP Client” in the list of Applications. Click on “EPP Client”.



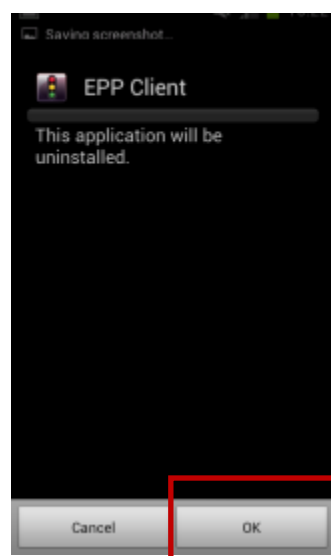
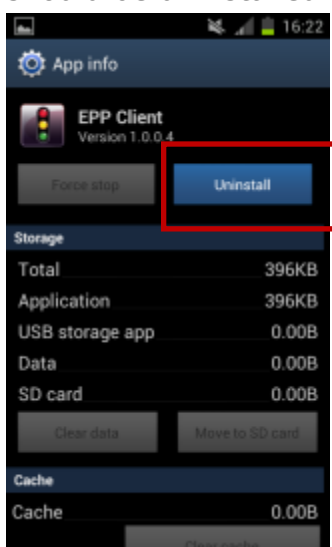
6. Click on "Force stop" and confirm the warning with "OK".



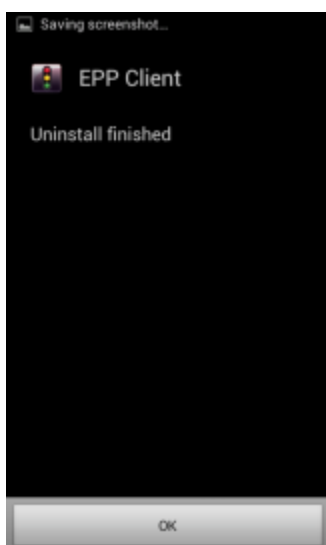
7. Now select "Clear data".



- Now click “Uninstall” and confirm with “OK” the question if EPP Client should be uninstalled.



- A message will indicate “Uninstall finished”, that the EPP Client was now uninstalled from the Android device. Click “OK” and the process is finalized.



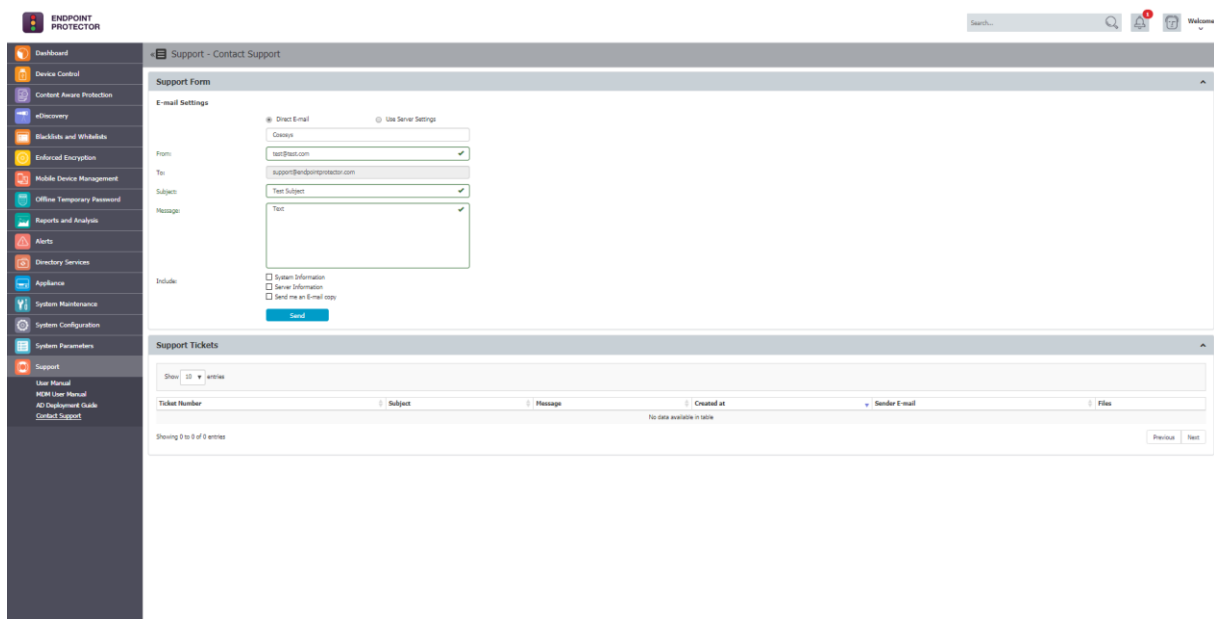
Note

Although the uninstallation can be performed by the user, the Endpoint Protector Appliance will also be notified about the removal of the Android EPP Client App.

16. Support

In case additional help, such as the FAQs or e-mail support is required, please visit our support website directly at <http://www.endpointprotector.com/support/>.

You can also write an e-mail to our Support Department under the Contact Us tab from the Support module.



The screenshot shows the Endpoint Protector web interface. On the left is a dark sidebar with a navigation menu including: Dashboard, Device Control, Content Aware Protection, eDiscovery, Blacklists and Whitelists, Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliances, System Maintenance, System Configuration, System Parameters, and Support. The 'Support' menu item is highlighted. The main content area is titled 'Support - Contact Support' and contains two sections. The top section is 'Support Form' with 'E-mail Settings'. It has radio buttons for 'Direct E-mail' (selected) and 'Use Server Settings'. Below are input fields for 'From' (set to 'User@test.com'), 'To' (set to 'support@endpointprotector.com'), 'Subject' (set to 'Test Subject'), and 'Message' (set to 'Test'). There are checkboxes for 'Include' system information, server information, and test on an e-mail only, with a 'Send' button below. The bottom section is 'Support Tickets', showing a 'Show 10 entries' dropdown and a table with columns for 'Ticket Number', 'Subject', 'Message', 'Created at', 'Sender E-mail', and 'Files'. The table is currently empty, displaying 'Showing 0 to 0 of 0 entries' and 'No data available in table'.

One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment, we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

17. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2019 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Android is registered trademark of Google Inc. Macintosh, Mac OS X, iOS, MacBook, are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.