



# ENDPOINT PROTECTOR

User Manual for Version 4.4.0.5

## Mobile Device Management (MDM) User Manual



## Table of Contents

<b>1.Introduction .....</b>	<b>1</b>
1.1. What is Endpoint Protector? .....	2
<b>2.Activation of Mobile Device Management ....</b>	<b>3</b>
2.1. Activation of Mobile Device Management Feature .....	4
<b>3.How Endpoint Protector MDM Works .....</b>	<b>5</b>
3.1. Supported Operating Systems and devices.....	6
<b>4.MDM Setup APNS (Apple) &amp; GCM (Google Android).....</b>	<b>7</b>
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.....	16
4.2.1. What is GCM (Google Cloud Messaging) and why I need it? .....	16
4.2.2. How to get your Google API Key for GCM and Maps?-new method (April 2014) .....	17
4.2.3. Entering Google API Key and Project Number in Endpoint Protector-new method .....	21
4.2.4. How to get your Google API Key for GCM and Maps?-old method .....	22
4.2.5. Entering Google API Key and Project Number in Endpoint Protector-old method .....	25
4.2.6. Google C2DM.....	26
<b>5.iOS EPP MDM App .....</b>	<b>27</b>
5.1. EPP MDM iOS App Supported iOS Versions .....	27
5.2. EPP MDM iOS App to locate devices .....	27
5.3. EPP MDM iOS App to enroll devices (optional).....	28
5.4. EPP MDM iOS App Device Information .....	28
5.5. Installing the EPP MDM iOS App .....	29
5.6. Allow Location Services for EPP MDM iOS App.....	30
5.7. Pushing and Managing EPP MDM App to iOS Devices .....	30

## 6. Android Endpoint Protector MDM Client App 31

- 6.1. EPP MDM Android Client App Supported Versions ..... 31
- 6.2. The Android EPP Client App ..... 31
- 6.3. EPP Client Android App to enroll devices ..... 31
- 6.4. Install EPP Client App on Android and Enrolling Android Device 32

## 7. Enrolling Mobile Devices ..... 38

- 7.1. Different Enrollment methods are available: ..... 39
- 7.2. Mobile Device Enrollment ..... 40
  - 7.2.1. iOS and OS X Enrollment and Profile Protection ..... 43
  - 7.2.2. iOS and OS X Profile Protection Deletion Passphrase ..... 44
  - 7.2.3. Sending E-Mail or SMS Enrollment Invitation (iOS/OS X / Android) 46
  - 7.2.4. SMS Enrollment Number Format (iOS / Android) ..... 46
  - 7.2.5. E-Mail Enrollment Invitation (iOS/OS X / Android) ..... 47
  - 7.2.6. SMS Enrollment Invitation (iOS / Android) ..... 48
  - 7.2.7. iOS and OS X Mobile Device Enrollment over URL ..... 49
  - 7.2.8. iOS Mobile Device Enrollment through EPP MDM App ..... 51
  - 7.2.9. Android Device Enrollment ..... 54
  - 7.2.10. Bulk Enrollment ..... 54

## 8. Managing Mobile Devices ..... 58

- 8.1. Mobile Device Status ..... 60
  - 8.1.1. Available Options ..... 63

## 9. Manage iOS Devices ..... 65

- 9.1. Security Settings (Security Profile) on iOS ..... 65
  - 9.1.1. Password / Passcode Setting on iOS Device ..... 66
  - 9.1.2. iOS Device Hardware Encryption ..... 66
- 9.2. Restrictions (Restrictions Profile) on iOS ..... 66
  - 9.2.1. The following iOS features can be restricted ..... 68
  - 9.2.2. The following Applications can be restricted ..... 68
  - 9.2.3. iCloud restrictions / Photo stream restrictions ..... 68
  - 9.2.4. Security and Privacy Restrictions ..... 69
  - 9.2.5. Content Rating Restrictions ..... 69
  - 9.2.6. iOS7 Restrictions ..... 70
  - 9.2.7. iOS8 Restrictions ..... 70

9.2.8. Supervised Device Restrictions .....	70
9.3. Remote iOS Lock/Wipe .....	71
9.3.1. Lock Device .....	71
9.3.2. Clear Passcode .....	71
9.3.3. Remote iOS Device Wipe (Device Nuke) .....	71
9.4. iOS Disable Device Password / Passcode .....	72
9.5. Device Ownership .....	72
9.6. Voice Roaming on iOS .....	72
9.7. Data Roaming on iOS .....	73
9.8. Profile Removal Policy for iOS Devices .....	73
9.9. Refresh Device Details for iOS .....	74
9.10.Refresh App List for iOS .....	74
9.11.Installed Apps on iOS .....	75
9.12.Refresh Profile List on iOS .....	75
9.13.Profiles on iOS Devices Information .....	75
9.13.1. Remove Profile from iOS Device .....	76
9.14.Manage WiFi on iOS .....	76
9.14.1. Wipe Wi-fi Settings .....	77
9.15.Manage Mail on iOS .....	77
9.15.1. Wipe E-mail Settings .....	77
9.16.Exchange Active Sync .....	77
9.17.Manage VPN on iOS .....	78
9.18.Manage APN settings on iOS .....	78
9.19.Manage Cellular Settings on Supervised iOS 7 devices .....	79
9.20.App Lock on Supervised iOS 7 devices .....	79
9.21.Installed Apps .....	80
9.22.History of iOS Devices Actions .....	80
9.23.History Location .....	81
<b>10. Manage OSX Devices .....</b>	<b>82</b>
10.1.Security Settings (Security Profile) on OS X .....	82
10.1.1. Password / Passcode Setting on OS X Device .....	83
10.1.2. OS X Device Hardware Encryption .....	83

10.2. File Vault 2 Disk Encryption on OS X .....	83
10.2.1. Disk Encryption Status.....	85
10.3. Remote Lock of Device .....	85
10.4. Remote OS X Device Wipe (Device Nuke).....	85
10.5. Device Ownership .....	86
10.6. Profile Removal Policy for OS X Devices .....	86
10.7. Refresh Device Details for OS X .....	87
10.8. Refresh App List for OS X.....	87
10.9. Installed Apps on OS X .....	87
10.10. Refresh Profile List on OS X .....	88
10.11. Profiles on OS X Devices Information .....	88
10.11.1. Remove Profile from OS X Device.....	88
10.12. Manage WiFi on OS X.....	89
10.12.1. Wipe Wi-fi Settings.....	89
10.13. Manage Mail on OS X .....	89
10.13.1. Wipe E-mail Settings .....	90
10.14. Manage VPN on OS X .....	90
10.15. History of OS X Devices Actions.....	91
<b>11. Manage Android Devices.....</b>	<b>92</b>
11.1. Security Settings (Security Profile) on Android.....	92
11.1.1. Password / Passcode Setting on Android Device .....	93
11.1.2. Device Password .....	94
11.1.3. Android Device Hardware Encryption .....	94
11.2. Request Storage Encryption .....	95
11.3. Remote Android Lock of Device.....	95
11.4. Remote Android Device Wipe (Device Nuke).....	96
11.4.1. Android Remote Wipe of SD-Card.....	96
11.5. Device Ownership .....	97
11.6. Android Device Location Settings .....	97
11.6.1. Location Accuracy Fine on Android .....	98
11.6.2. Location Cost Allowed on Android.....	98
11.7. Manage Wifi .....	98

11.8. Manage Bluetooth .....	98
11.9. Manage Camera on Android .....	99
11.10. Play Sound on Device for Android .....	99
11.11. Refresh Google Accounts for Android .....	100
11.12. Refresh Device Details for Android .....	100
11.13. Refresh App List for Android .....	100
11.14. Manage Calendar Events .....	101
11.15. Installed Apps on Android .....	102
11.15.1. Removing Installed Apps on Android .....	102
11.16. Get Contacts on Android .....	103
11.17. Get Accounts on Android .....	103
11.18. History of Android Device Actions .....	103
11.19. Manage WiFi, Manage Mail, Profiles on Android .....	104
<b>12. Mobile Application Management (MAM) for iOS .....</b>	<b>105</b>
12.1. Adding Apps to your Managed Apps Catalog .....	106
12.1.1. Searching for Apps .....	106
12.1.2. Adding Apps to Managed Apps Catalog .....	107
12.1.3. Adding „Enterprise Apps“ to Managed Apps Catalog .....	107
12.2. Editing App Management Options .....	108
12.3. Managed Paid Apps .....	110
12.4. Pushing Apps to iOS Devices .....	112
12.4.1. Update Managed Apps / Changing Settings .....	113
12.5. Removing Managed Apps from iOS Devices .....	114
<b>13. Android App Management .....</b>	<b>115</b>
13.1. Adding Apps to your Managed Apps Catalog .....	116
13.2. Editing App Management Options .....	116
13.3. Pushing Apps to Android Devices .....	117
13.4. Removing Managed Apps from Android Devices .....	118
<b>14. Policy Builder for iOS, OSX or Android Devices .....</b>	<b>119</b>

14.1.Create a Policy for iOS, OS X or Android Devices.....	120
14.2.Assigning Devices to Policy.....	121
<b>15. Unmanage a Mobile Device / Uninstall App</b>	<b>122</b>
15.1.iOS and OS X Device Unmanage by Administrator (over-the-air)	122
15.1.1. iOS Uninstall / Unmanage by User (on Device) .....	122
15.1.2. OS X Uninstall / Unmanage by User (on Device) .....	123
15.2.Uninstall iOS EPP MDM app .....	123
15.3.Android EPP Client App Uninstall / Unmanage Android Device	123
<b>16. GeoFencing .....</b>	<b>128</b>
16.1.How to setup a GeoFence.....	129
16.2.How to deploy MDM Policies using Geofences .....	130
<b>17. Installing Root Certificate to your Internet Browser .....</b>	<b>131</b>
17.1.For Microsoft Internet Explorer .....	131
17.2.For Mozilla Firefox .....	139
<b>18. Terms and Definitions .....</b>	<b>141</b>
18.1.Server Related.....	141
18.2.Client Related .....	142
<b>19. Support .....</b>	<b>143</b>
<b>20. Important Notice / Disclaimer.....</b>	<b>144</b>

# 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.

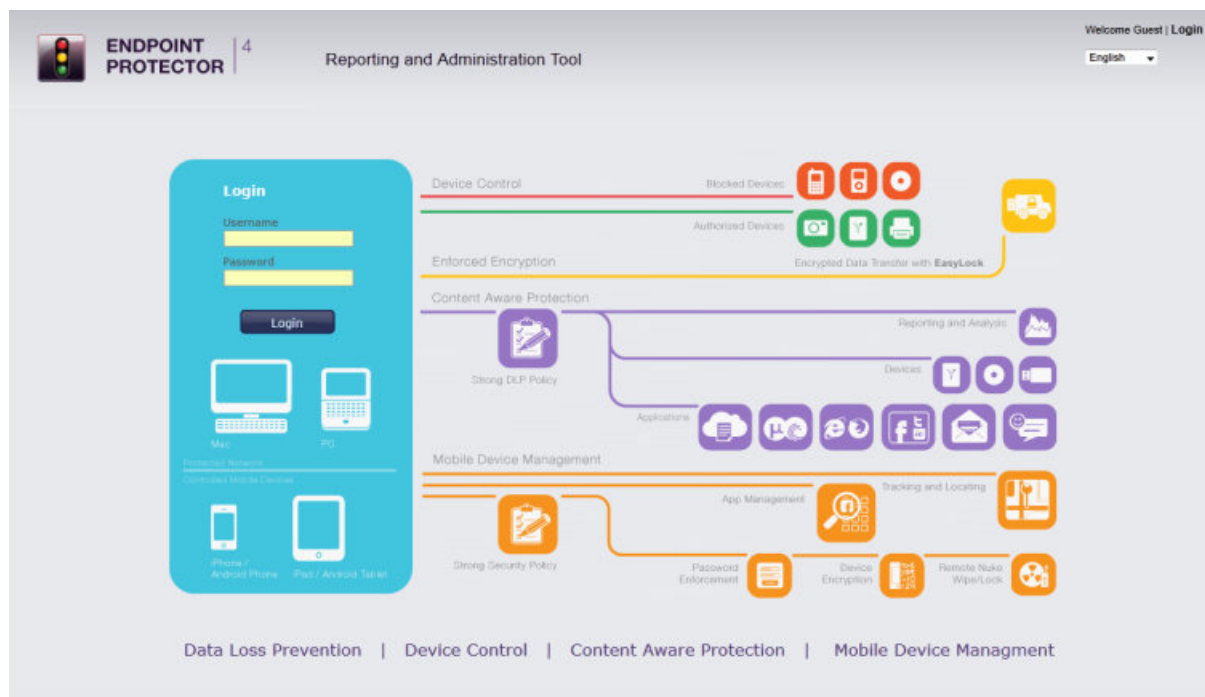
The wide adoption of the BYOD (Bring-Your-Own-Device) model by companies worldwide led to the use of more personal mobile devices by employees for storing business information together with private data such as photos and music. This trend raised new issues for IT administrators, which are faced now 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.

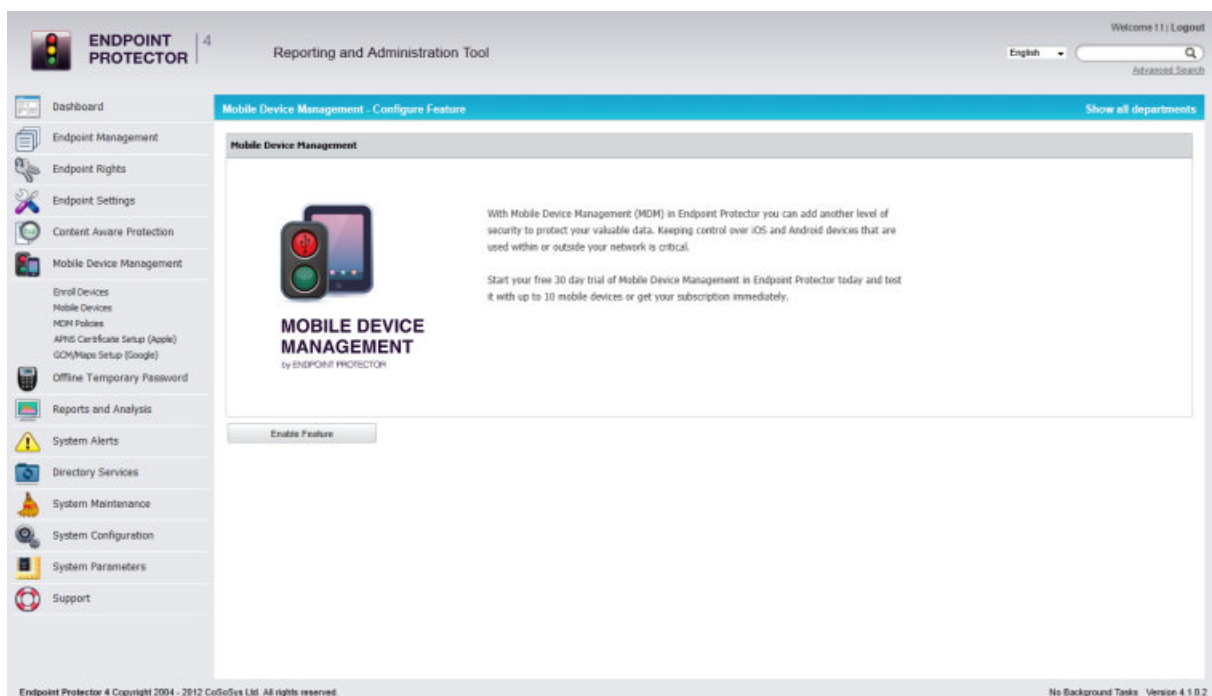


Endpoint Protector comprises three separate modules, which used together ensures the next generation security of your endpoints:

- **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.



## 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.

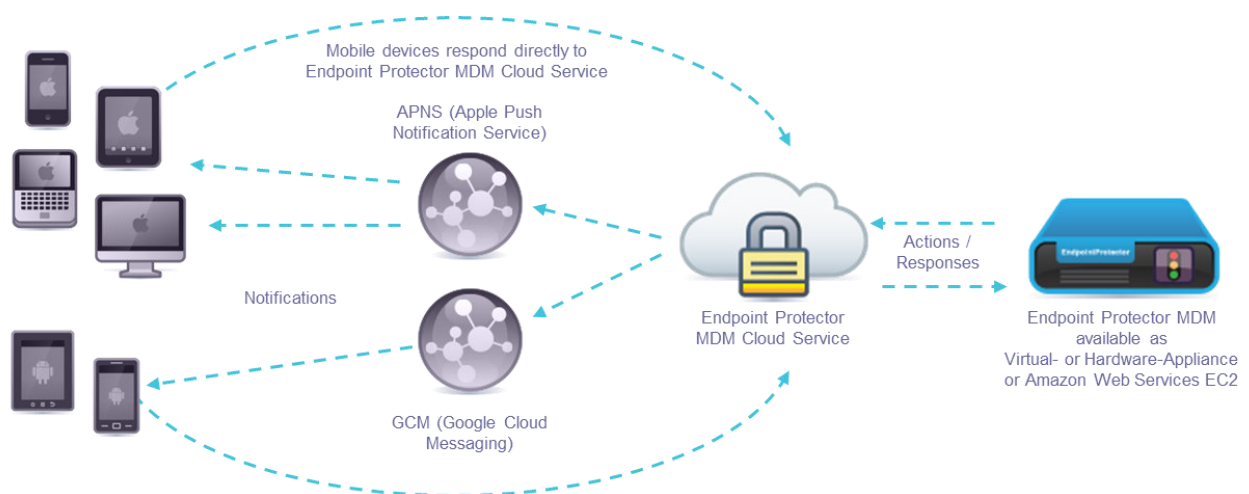
Please make sure your Firewall will have domains @cososys.com and @endpointprotector.com whitelisted for you to receive all communication.

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:

- iOS7 (iPhone and iPad), iOS6 (iPhone and iPad), iOS5, iOS4
- OS X 10.9.1+
- Android 2.2+ (Codename Froyo) or newer versions

A list of supported Android mobile devices is not provided due to the large number of devices from different manufacturers. In general Android devices with Android Operating version 2.2 and newer are supported.

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

Before you can use the Endpoint Protector MDM features for iOS, OS X and Android different settings are required for you to make. The following steps describe the steps and settings needed to be able to communicate between your mobile devices and Endpoint Protector.

### **Attention!**

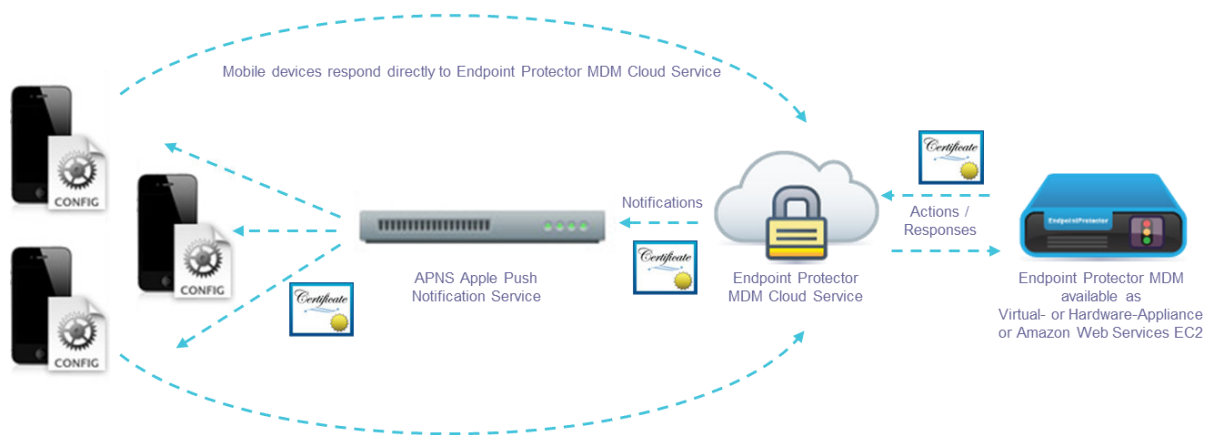
For Endpoint Protector Administrators that want to use the MDM Functionality only with Android devices the Apple APNS Setup (required for MDM with iOS or OS X) is **NOT REQUIRED**. If you want to use Endpoint Protector MDM with iOS/ OS X and Android devices the setup of both GCM (Google Cloud Messaging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

**Endpoint Protector 4** Reporting and Administration Tool

**Mobile Device Management - APNS Certificate Enrollment**

**Information**

To use Mobile Device Management features for iOS devices it is required that you follow the steps below for the setup and agree and comply to the Apple License Terms for Mobile Device Management (MDM) from step 2 below.

**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

**Step 2 - Request your signed certificate for APNS from Apple**

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. At this step provide Apple with the certificate you have download above.

**Step 3 - Upload certificate signed by Apple**

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

Browse for APNS certificate signed by Apple:

Endpoint Protector 4 Copyright 2004 - 2012 CoSoSys Ltd. All rights reserved.

#### 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 (Firefox or Safari browser, not Internet Explorer!) 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](https://cloud.endpointprotector.com) in order to enable Mobile Device Management for iOS.

Browse for APNS certificate signed by Apple:

Browse...

Upload

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 shows the Endpoint Protector interface with the 'Mobile Device Management - APNS Certificate Enrollment' section highlighted. A green status bar at the top of this section indicates: 'Your Apple APNS Certificate is already enrolled and it will expire on 12 Mar 2014 10:48:38.' Below this, a note states: 'Your APNS certificate must be renewed with Apple before its expiration date. Renewing it in time does not require you to re-enroll devices. Note, if your APNS certificate expires, is revoke or you create a new certificate, each device will have to be re-enrolled.' The interface then presents three steps: Step 1 - Fill in this form below with your company information for a CSR (with fields for Company Name, E-mail, Country, State or Province Name, and Location (City)); Step 2 - Request your signed certificate for APNS from Apple (with instructions to visit the Apple website); and Step 3 - Upload certificate signed by Apple (with a 'Browse...' button to select the certificate file 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.

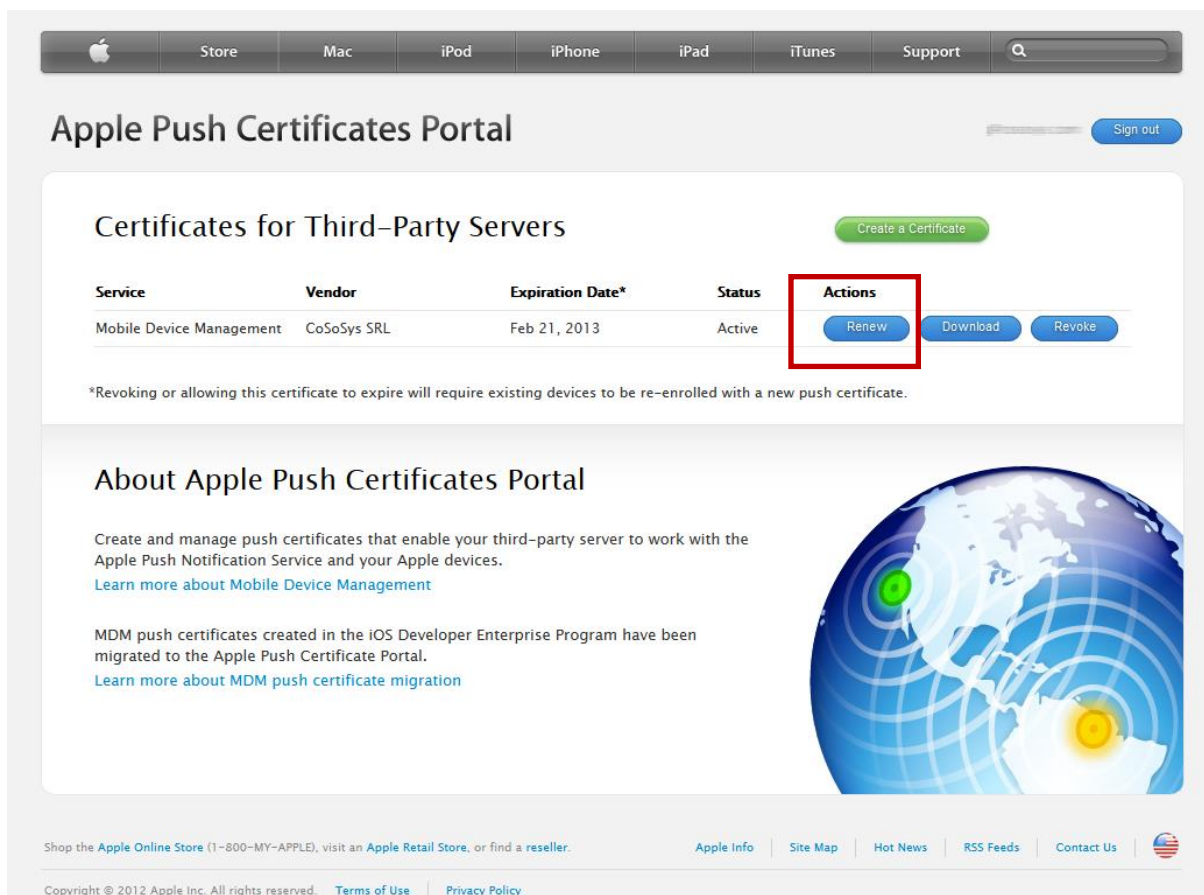
#### Note!

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 displays the Apple Push Certificates Portal. At the top, there is a navigation bar with links to Store, Mac, iPod, iPhone, iPad, iTunes, and Support. Below this, the main heading is "Apple Push Certificates Portal". A "Sign out" button is visible in the top right corner.

The main content area is titled "Certificates for Third-Party Servers". It features a table with the following columns: Service, Vendor, Expiration Date\*, Status, and Actions. The table contains one entry for "Mobile Device Management" with a vendor of "CoSoSys SRL" and an expiration date of "Feb 21, 2013". The status is "Active". In the "Actions" column, there are 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."

The bottom section of the page is titled "About Apple Push Certificates Portal". It contains text explaining the purpose of the portal and provides links to "Learn more about Mobile Device Management" and "Learn more about MDM push certificate migration".

The footer includes links to the Apple Online Store, Apple Retail Store, and a reseller, along with links to Apple Info, Site Map, Hot News, RSS Feeds, and Contact Us. It also includes a copyright notice for 2012 Apple Inc. and links to Terms of Use and Privacy Policy.

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.

**Apple Push Certificates Portal**

**Renew Push Certificate**

Enter your Certificate Signing Request signed by your third-party server vendor to renew the following push certificate.

Service: Mobile Device Management  
Vendor: CoSoSys SRL

**Browse...**

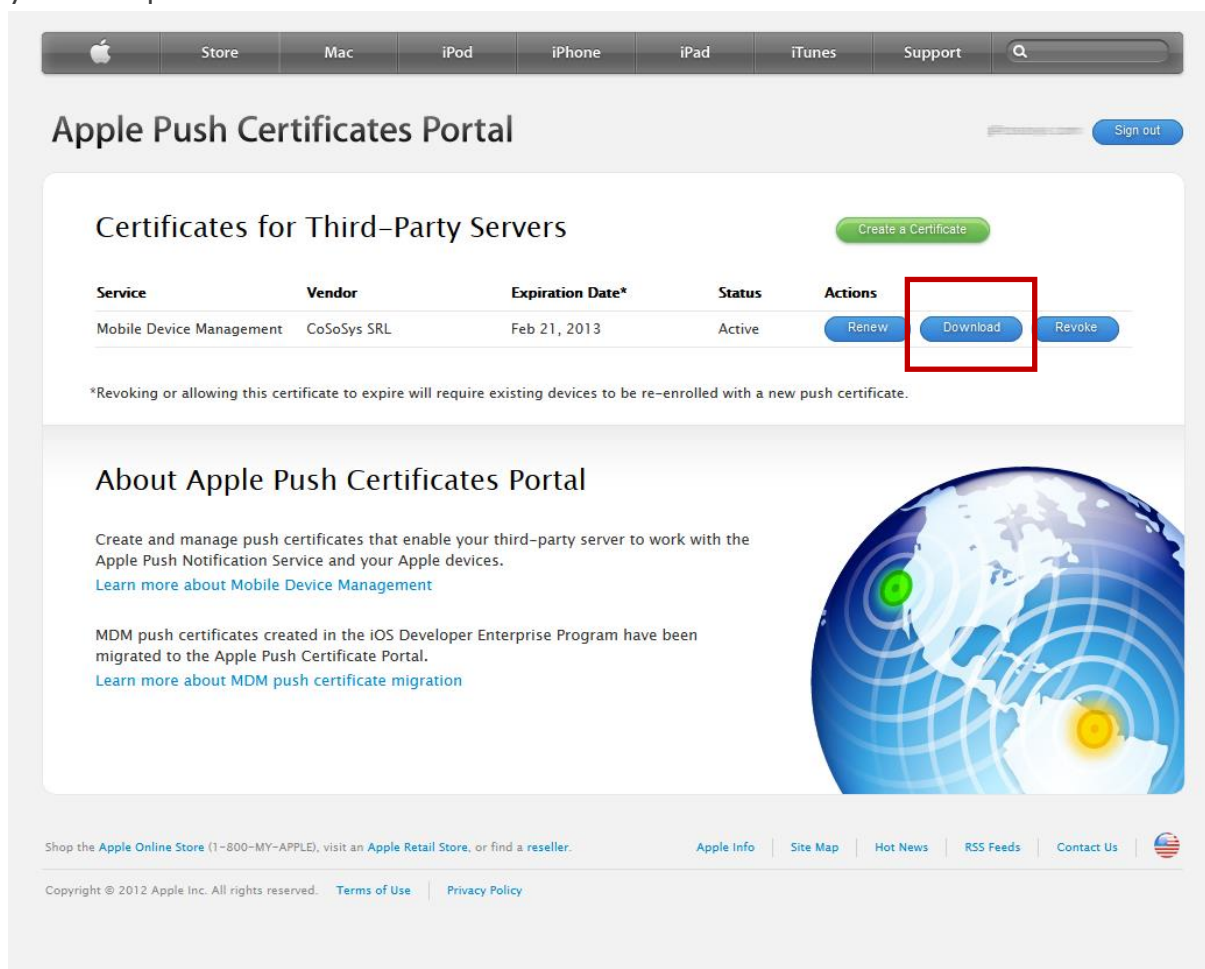
**Cancel** **Upload**

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](#)

- 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	<a href="#">Renew</a> <a href="#">Download</a> <a href="#">Revoke</a>

\*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](https://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/>

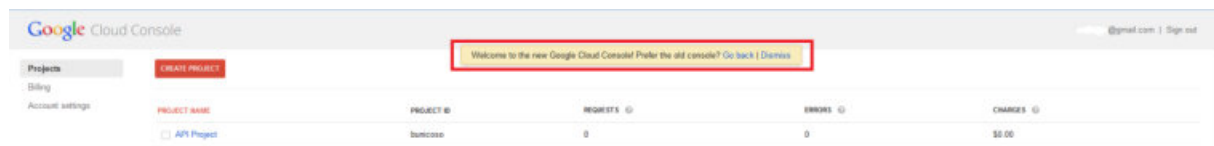
### 4.2.2. How to get your Google API Key for GCM and Maps?-new method (April 2014)

Visit the following site, Google Cloud Console, and login with your company Google account.

<https://cloud.google.com/console>

#### Note!

The old method can still be used by those who prefer it over the new. When you log in with your Google account to the console, you have the option to revert to the old style. To set up GCM with the old method, see paragraph 4.2.4 and 4.2.5.

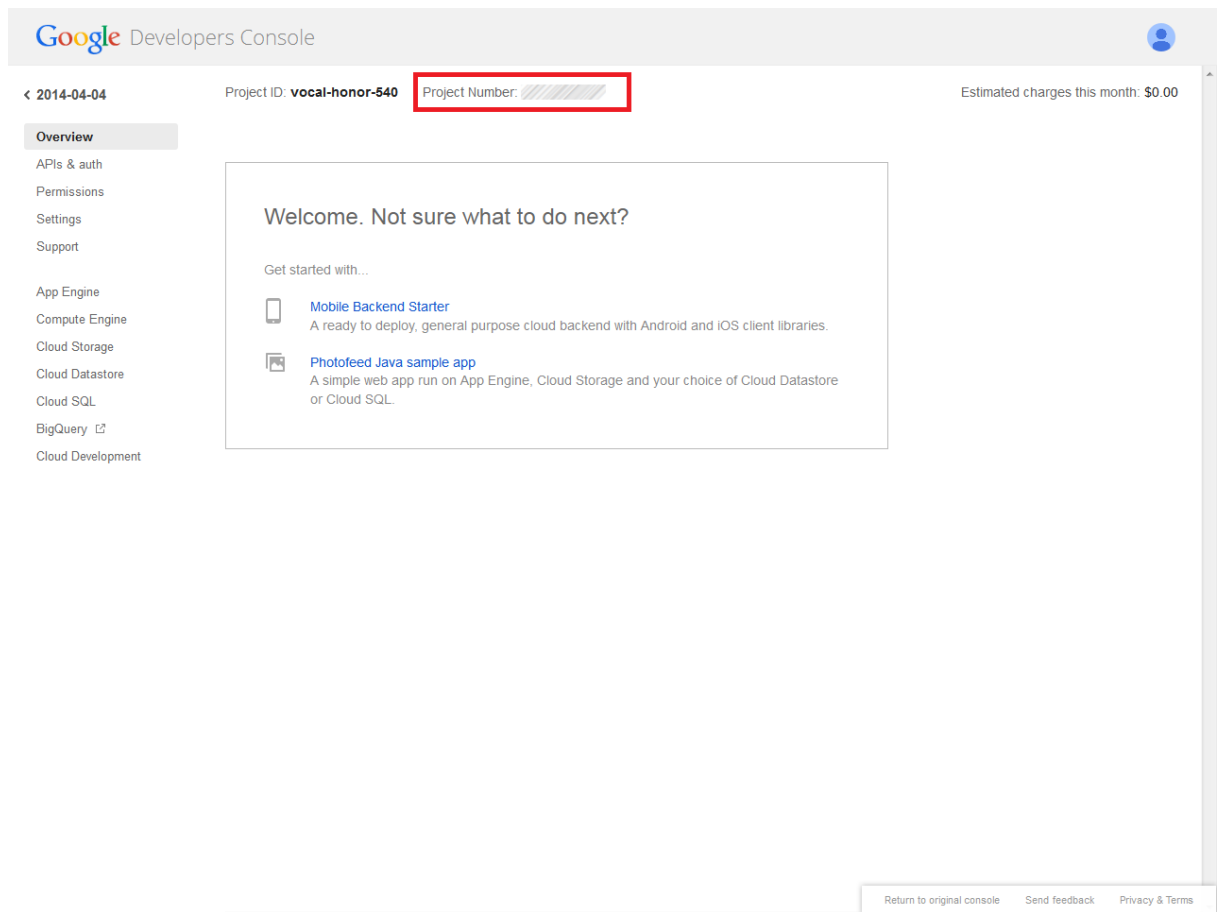


1. If you login to the Google Cloud Console for the first time you will be asked to "CREATE PROJECT". Select this option and give the project a name.

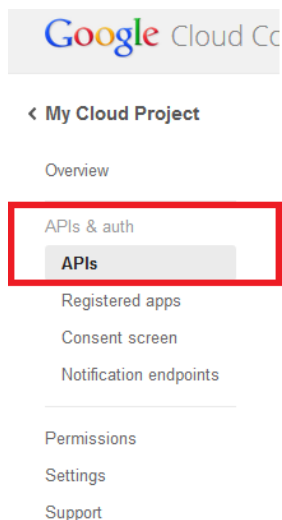




- The Project will be given a Project Number by Google which you need to enter in the Endpoint Protector interface as described in the next paragraph.



- In the left menu go to APIs & auth > APIs .

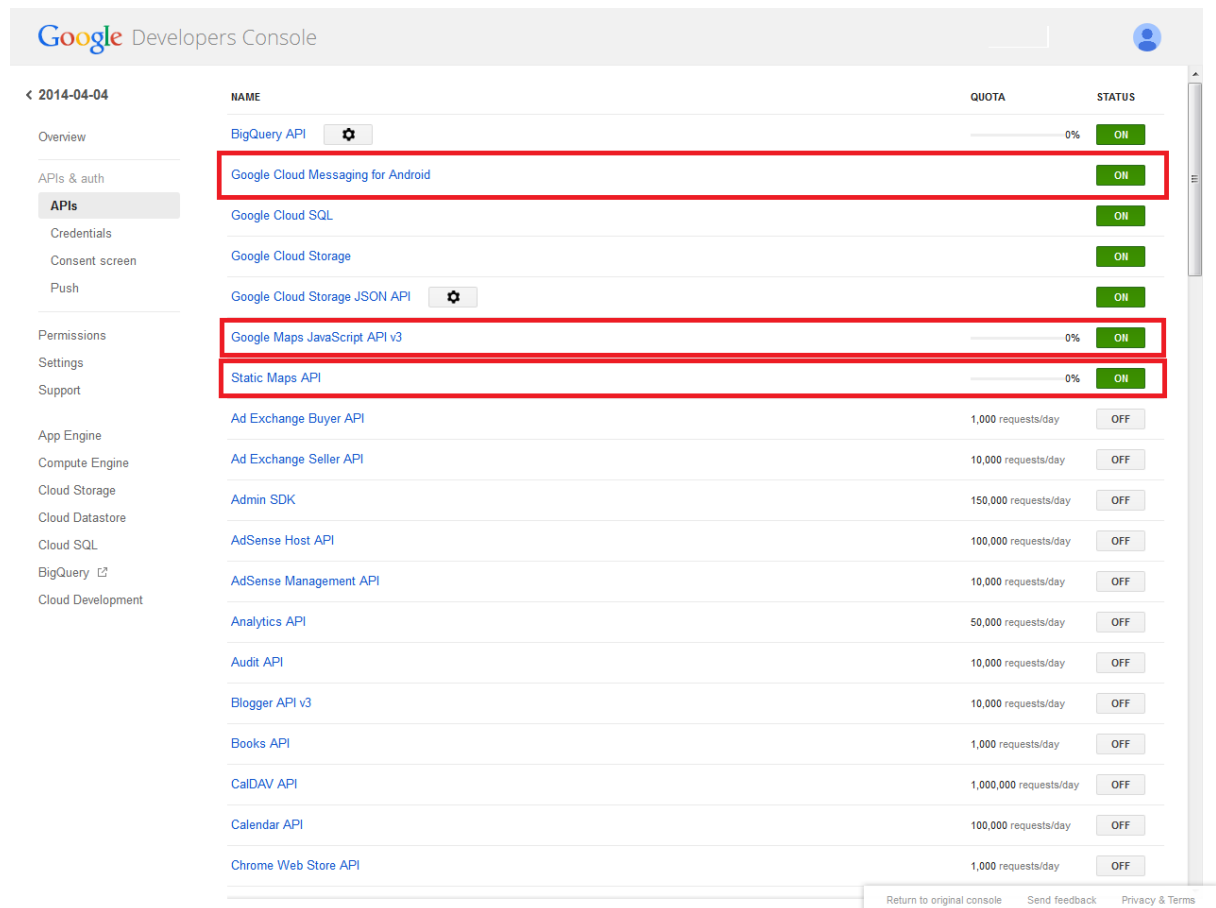


- Make sure the following three Google Services have ON status (green):

- Google Cloud Messaging for Android,**

- **Google Maps JavaScript API v3,**
- **Static Maps API.**

To enable these three services toggle it to the status ON.



Google Developers Console

< 2014-04-04

Overview

APIs & auth

**APIs**

Credentials

Consent screen

Push

Permissions

Settings

Support

App Engine

Compute Engine

Cloud Storage

Cloud Datastore

Cloud SQL

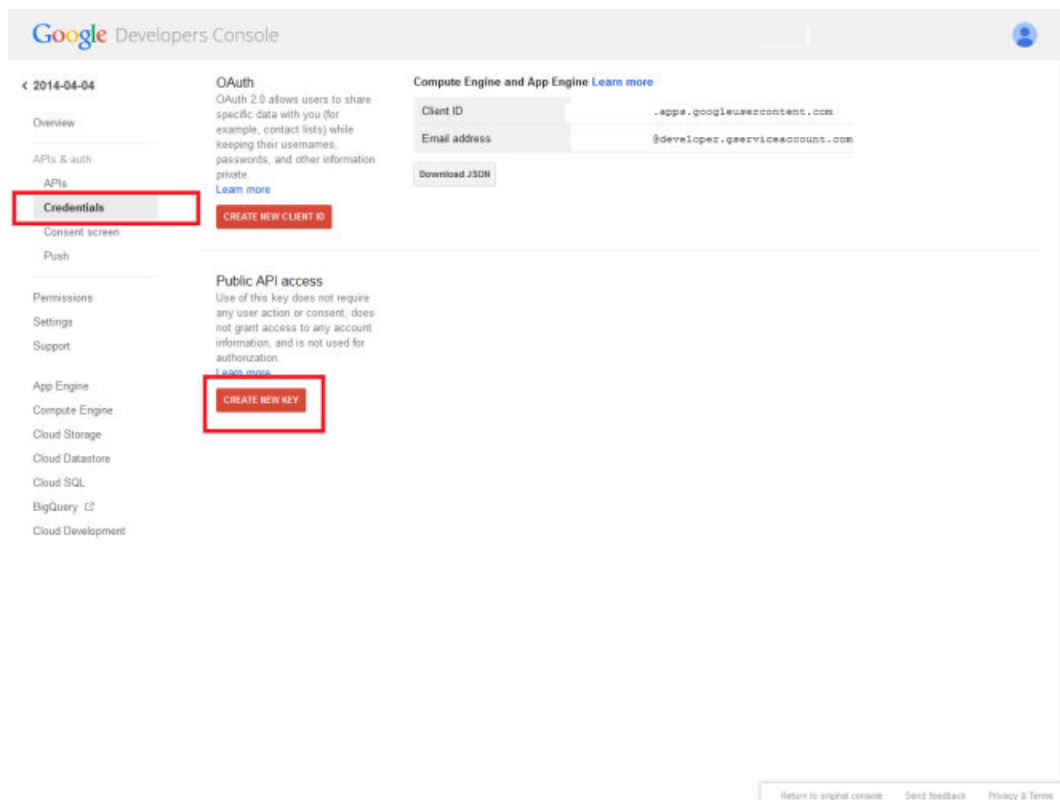
BigQuery

Cloud Development

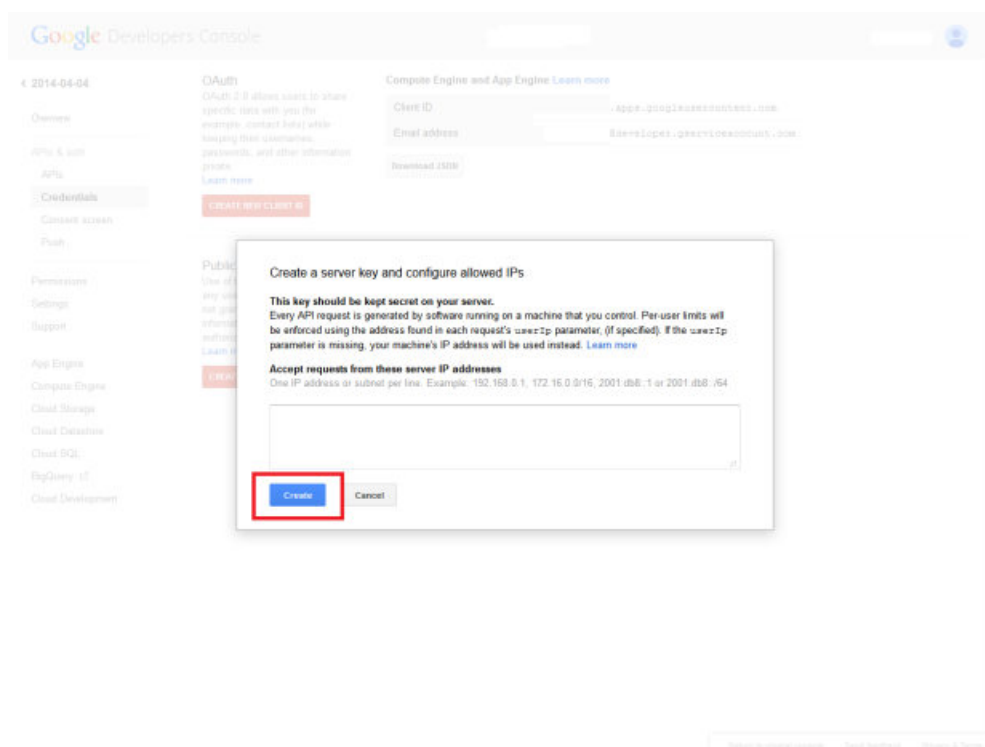
NAME	QUOTA	STATUS
BigQuery API	0%	ON
Google Cloud Messaging for Android		ON
Google Cloud SQL		ON
Google Cloud Storage		ON
Google Cloud Storage JSON API		ON
Google Maps JavaScript API v3	0%	ON
Static Maps API	0%	ON
Ad Exchange Buyer API	1,000 requests/day	OFF
Ad Exchange Seller API	10,000 requests/day	OFF
Admin SDK	150,000 requests/day	OFF
AdSense Host API	100,000 requests/day	OFF
AdSense Management API	10,000 requests/day	OFF
Analytics API	50,000 requests/day	OFF
Audit API	10,000 requests/day	OFF
Blogger API v3	10,000 requests/day	OFF
Books API	1,000 requests/day	OFF
CalDAV API	1,000,000 requests/day	OFF
Calendar API	100,000 requests/day	OFF
Chrome Web Store API	1,000 requests/day	OFF

Return to original console Send feedback Privacy & Terms

5. In the left menu go to Credentials. Create a new key. When prompted choose the Server key option.



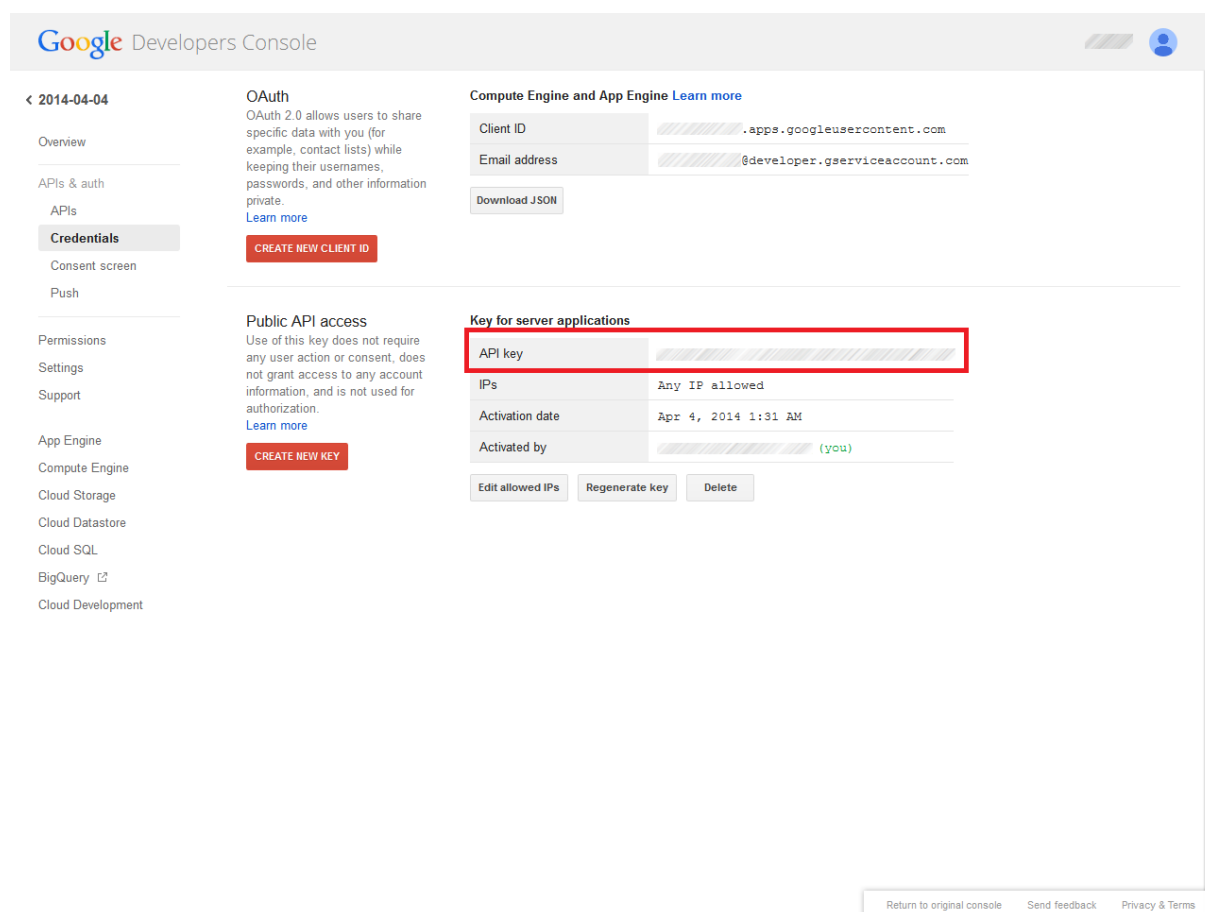
6. Press Create, leaving the "Accept requests from these server IP addresses" field blank.



7. You can now locate your API key under the “Key for server applications” section.

The API key has the following format (Example API key):

ExampleE67QWuu26-5j6WEEfWqgqYYouW1408-7



8. Copy the Google API key as described in the next paragraph in the Endpoint Protector interface.

#### 4.2.3. Entering Google API Key and Project Number in Endpoint Protector-new method

After you have obtained your Google API Key please enter it together with the Google Project Number in the Endpoint Protector Interface.

The Google Project Number you find on the Google Cloud Console Site under Projects > Overview > Project Number (paragraph 4.2.2, step 2).

The Server API Key you find on the Google Cloud Console Site under Projects > New Project> APIs & auth > Credentials > Key for server applications (paragraph 4.2.2, step 7).

Add them at Mobile Device Management > GCM/Maps Setup (Google).

The screenshot shows the 'Mobile Device Management - Configure Feature' page in the Endpoint Protector interface. The left sidebar contains navigation links for Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Desktops, Email Devices, Mobile Devices, MDM Policies, iOS App Management, APNS Certificate Setup (Apple), GCM/Maps Setup (Google), Offline Temporary Password, Reports and Analytics, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area has a blue header bar with the title and a 'Show all departments' link. Below this is an 'Information' section with a note about API key requirements. The 'Step 1 - Obtain API key from Google' section lists four steps. The 'Step 2 - Enter Google API key' section has a text input field with the value 'Example: AIzaSyD8-S61EEFmgFroul340B-7'. The 'Step 3 - Enter Google Project Number' section has a text input field with the value '112230440586'. A 'Save' button is at the bottom of the form.

After entering/copying the API Key and the Google Project Number press the “Save” button.

Once these steps were completed you can start enrolling Android devices to Endpoint Protector Mobile Device Management.

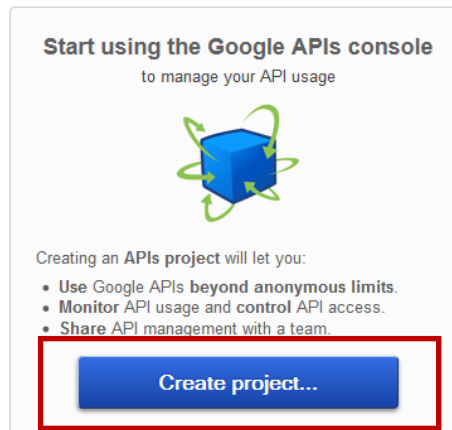
#### 4.2.4. How to get your Google API Key for GCM and Maps?-old method

Visit the following Google Site Google APIs Console and login with your company Google account.

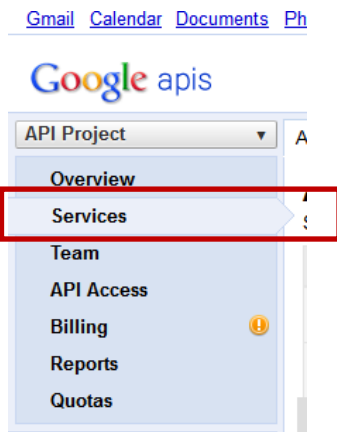
<http://code.google.com/apis/console>

1. If you login to the Google APIs Console for the first time you will be asked to “Create project...”. Select this option and give the project a name. The Project will be given a Project Number by Google which you also need to enter in the Endpoint Protector interface as described in the next paragraph).

Google apis



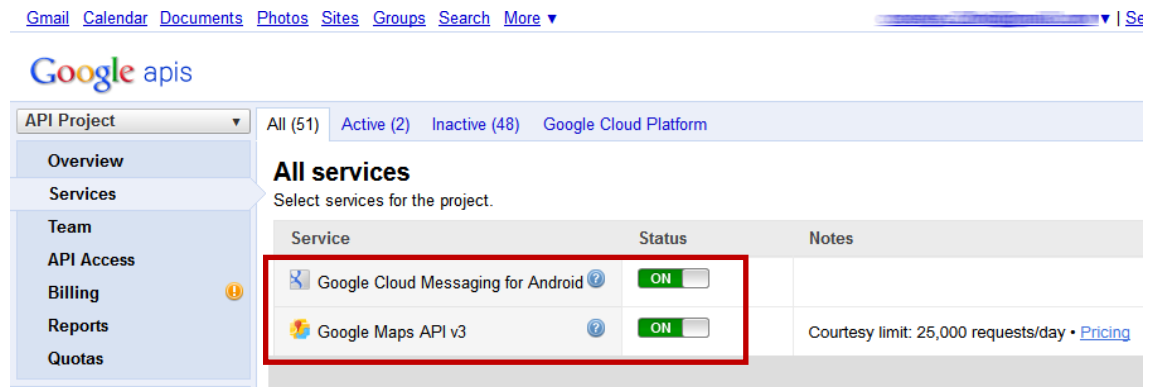
2. In the left menu on the Google APIs Console Site go to Services.



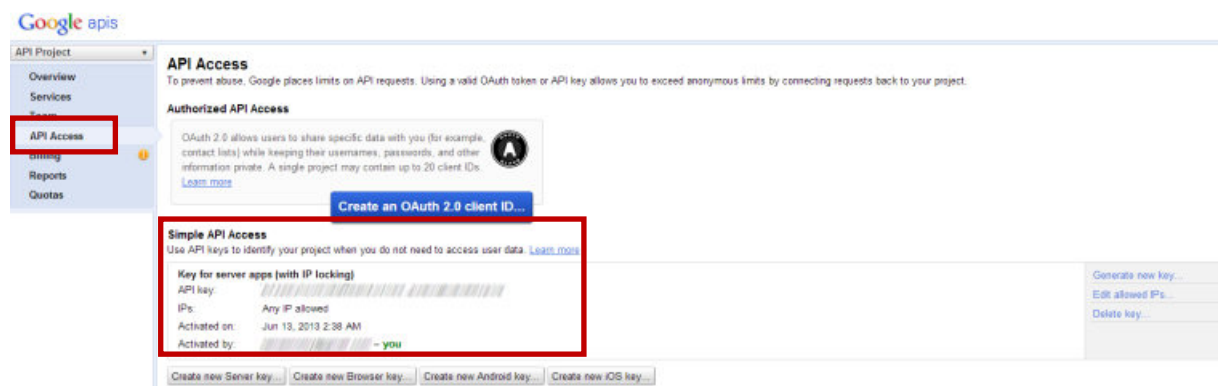
3. Make sure the following two Google Services have ON status (green):

- **Google Cloud Messaging for Android,**
- **Google Maps API v3.**

To enable these two services toggle it to the status ON, Google will ask you to agree to their Terms of Service/End User License Agreement.



4. You can now locate your API key in the left menu on the Google APIs Console Site under API Access > Simple API Access > API key.  
The API key has the following format (Example API key):  
ExampleE67QWuu26-5j6WEEfWqgqYYouW1408-7

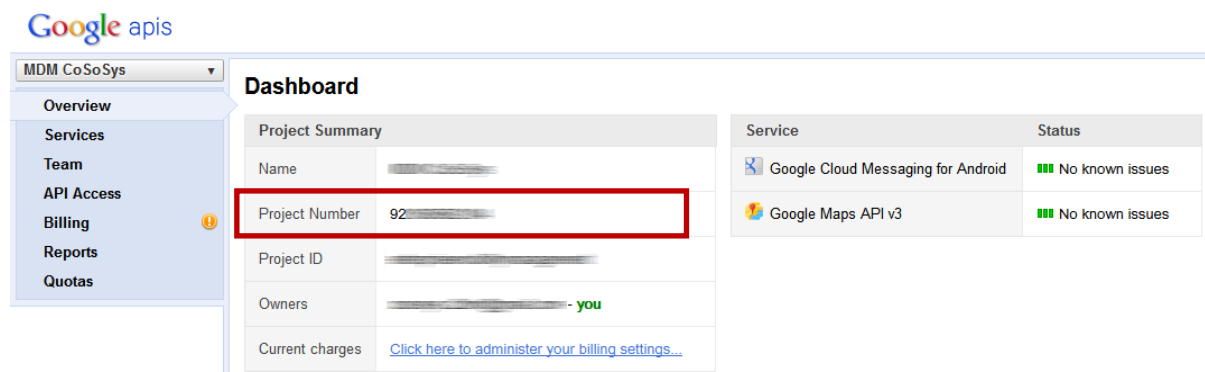


5. On the Google APIs Console Site in API Access > Simple API Access > you can also add referrers that are allowed to use your API keys, and we recommend you to add the following two. Do this by clicking on the right side next to the API key on "Edit allowed referrers..." and add there in separate lines:  
cloud.endpointprotector.com  
endpointprotector.com
6. Copy the Google API key as described in the next step in the Endpoint Protector interface.

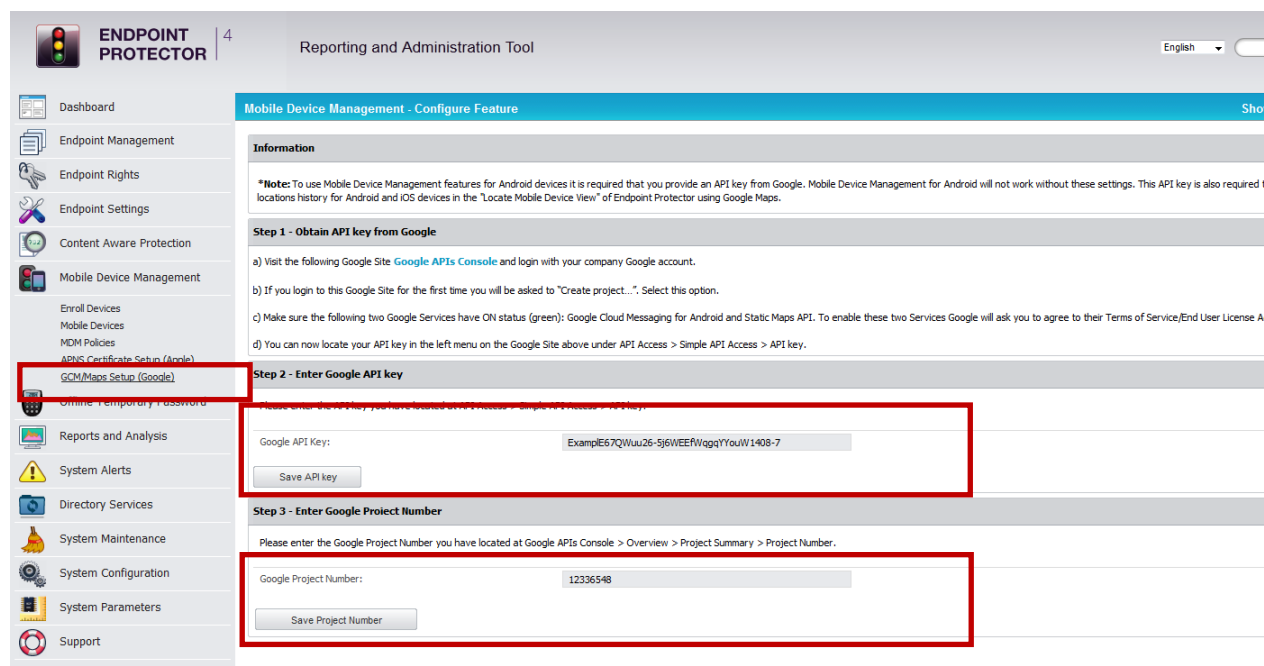
### 4.2.5. Entering Google API Key and Project Number in Endpoint Protector-old method

After you have obtained your Google API Key please enter it together with the Google Project Number in the Endpoint Protector Interface.

The Google Project Number you find on the Google APIs Console Site under > Overview > Project Number.



Add them at Mobile Device Management > GCM/Maps Setup (Google).



After entering/copying the API Key click "Save API Key".

Now enter the Google Project Number and click "Save Project Number".

After completing these steps you can start enrolling Android devices to Endpoint Protector Mobile Device Management.



#### 4.2.6. 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.

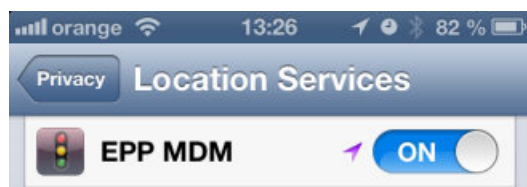
To start the EPP MDM app simply locate it on your iOS device home screen and click to start it.



## 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 devices 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.

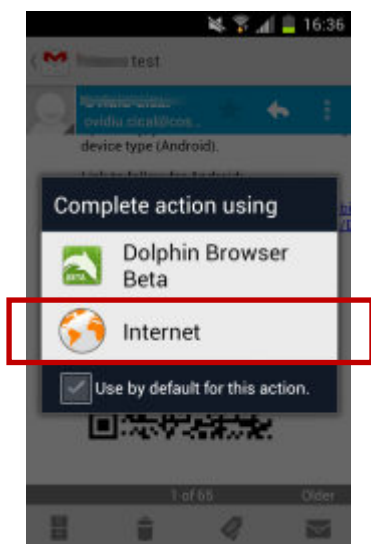
### 6.3. EPP Client Android App to enroll devices

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

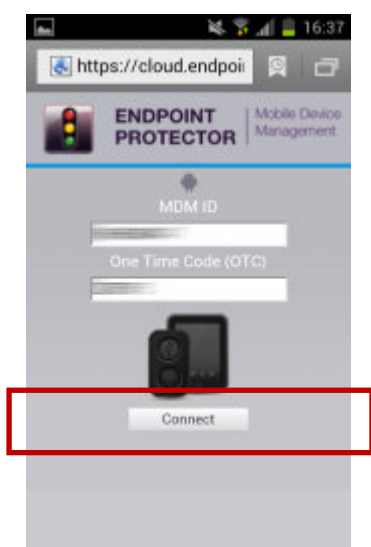
After receiving the enrollment invitation E-Mail or SMS click on the link provided in the E-Mail or SMS.

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



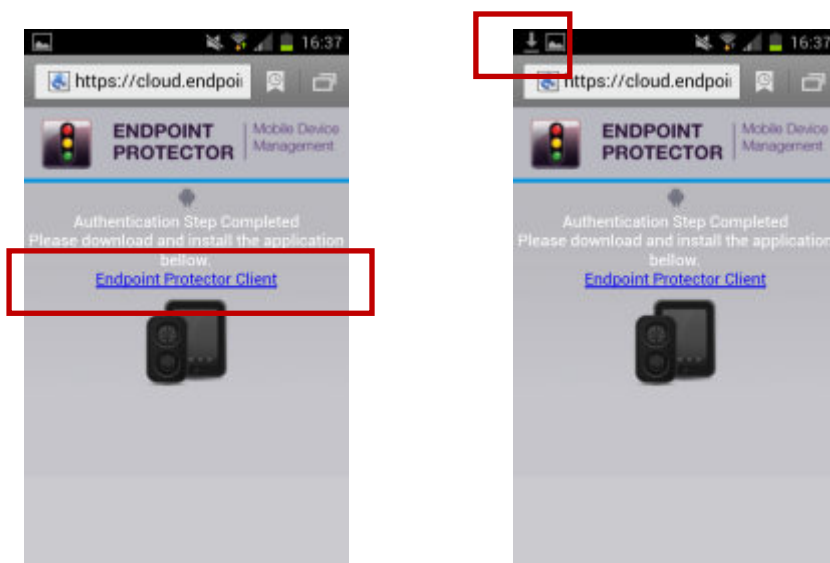
In this case (screenshot above) the choice for native browser is the option “Internet”, not the Dolphin or any other browser that might be installed on your Android device.

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).

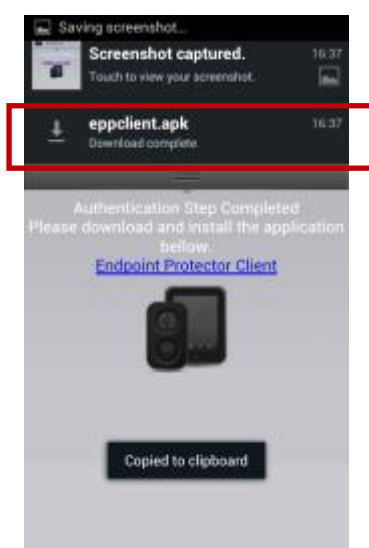


Click “Connect” to proceed”

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.

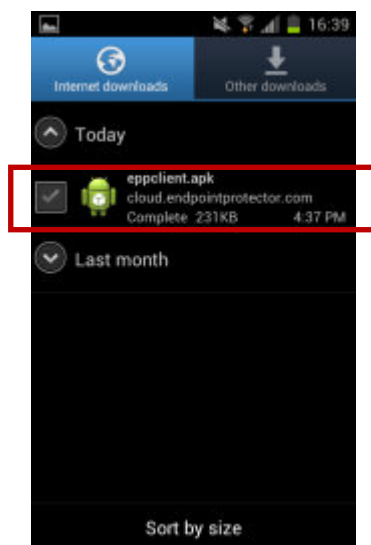


4. The download of the eppclient.apk (name of the EPP Client Android app download file) should finish rather fast depending on your data connection speed since the eppclient.apk is small.

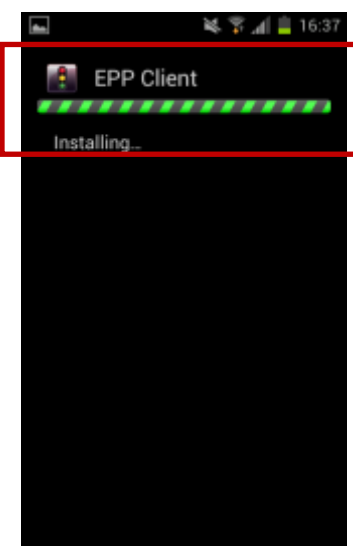
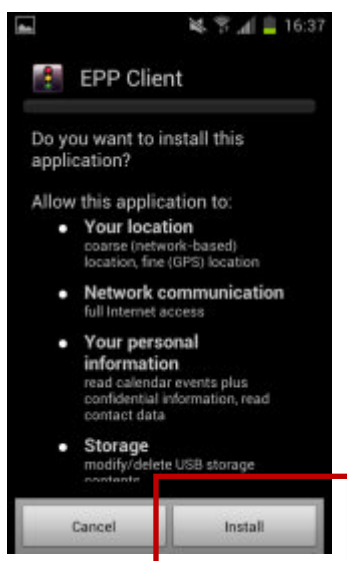




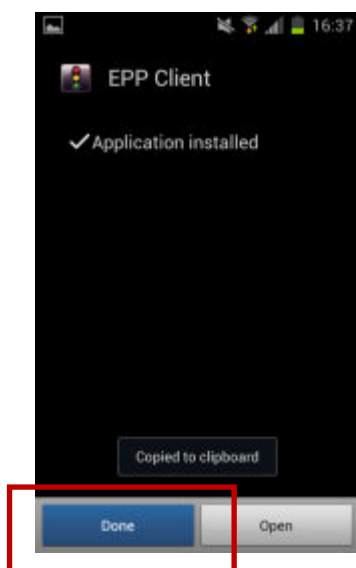
5. Locate now the `epclient.apk` in the download folder on your device.



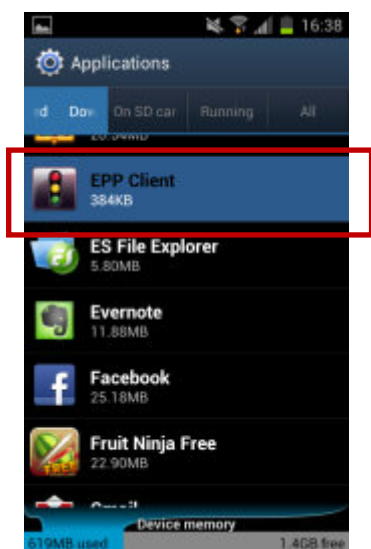
6. Click on the `epclient.apk` and select "Install". The EPP Client will start to install itself on the Android device.



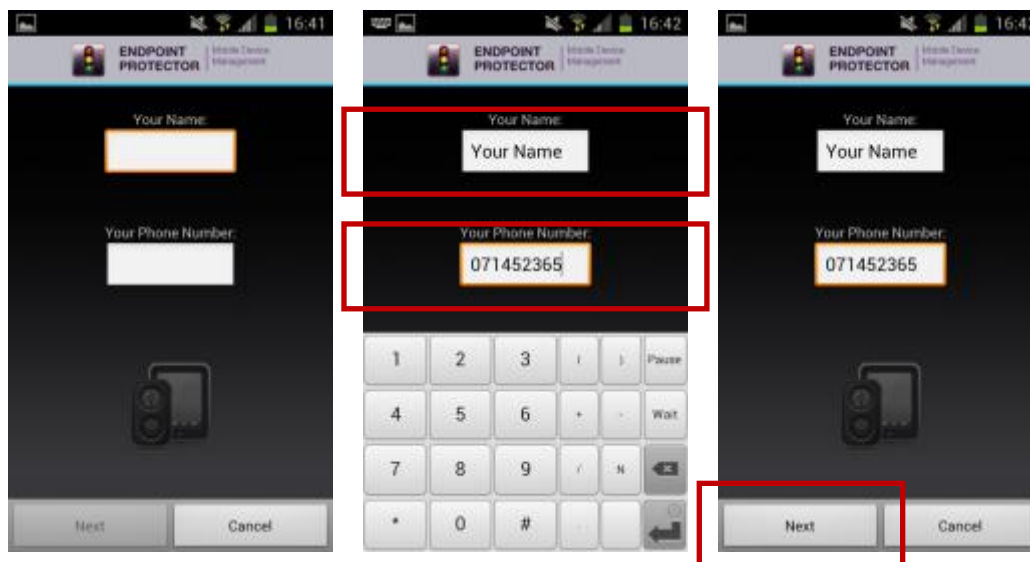
7. After the installation you will see a message indicating the installation is finished. Click “Done” to complete the final steps for your Android device enrollment.



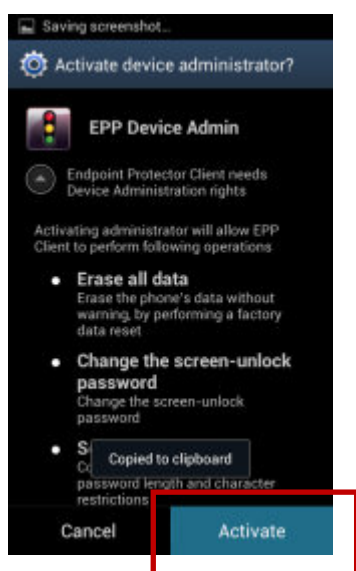
8. Go to “Applications” on your Android device. There locate the EPP Client and start it.



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.



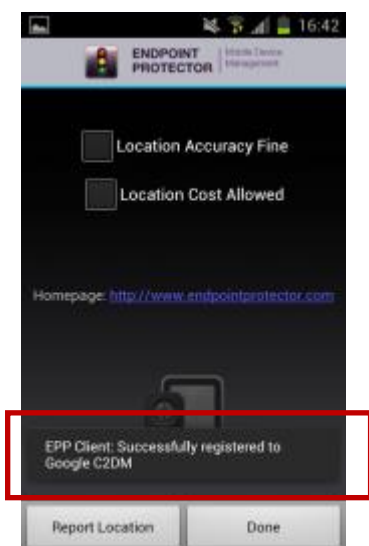
10. Now the question regarding device administration will appear which needs to be confirmed by clicking “Activate”.



### Attention!

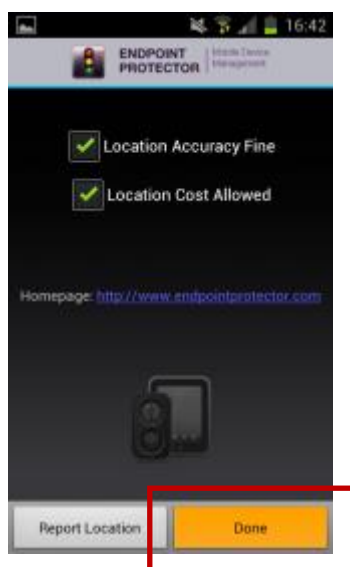
By not enabling this option, the Android mobile device cannot be remotely administrated / managed.

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.

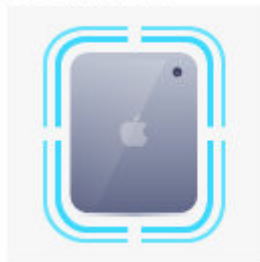


These two settings are described in the chapter 11.6.1 Location Accuracy Fine on Android 11.6.2 Location Cost Allowed on Android.

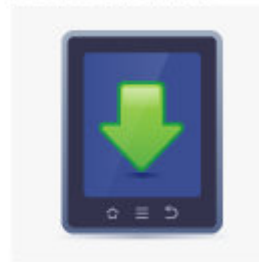
# 7. Enrolling Mobile Devices

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

### **Attention!**

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 'Endpoint Protector' Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Enroll Devices (highlighted with a red box), MDH Policies, APNS Certificate Setup (Apple), GCM/Maps Setup (Google), Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Mobile Device Management - Enroll Devices' and includes a 'Show all departments' link. It features three main sections: 'Mobile Device Management Information' showing 'Your MDM ID is:' (highlighted with a red box) and 'Currently managing:' (3 Mobile Devices); 'Enroll Mobile Devices' with instructions for iOS/iOS X/Apple and Android, and buttons for 'Send E-mail Request' and 'Send SMS Request'; and 'One Time Codes' with a table of results. The table has columns for 'Code', 'Uninstall Passphrase (Show)', and 'Actions'. It shows 12 results with a pagination control set to 10 per page. At the bottom, there are buttons for 'View Invitations Sent', 'View Available OTC', and 'Request More OTC'.

Code	Uninstall Passphrase (Show)	Actions
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]
XXXXXXXXXX	XXXXXXXXXX	[X]

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.

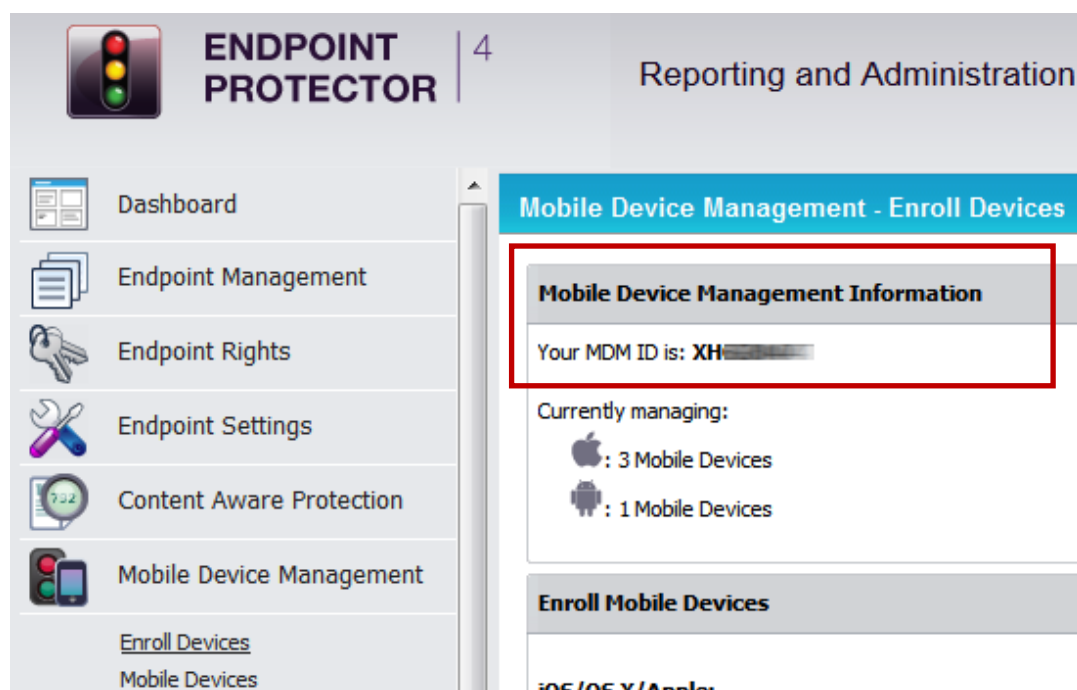
The enrollment of iOS, OS X and Android devices is similar in many ways. There are different enrollment options for each mobile device type available. The first two options allow the sending of E-mail and SMS based invitation requests to mobile devices, invitations which include short instructions on 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





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:

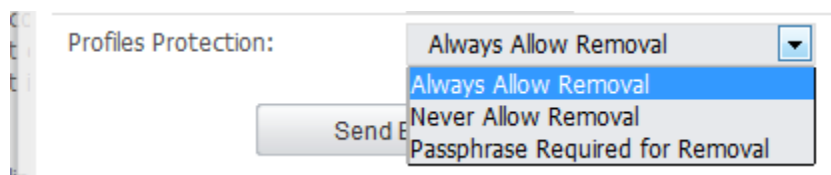
- using the "Reserve" right-click menu option 

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.

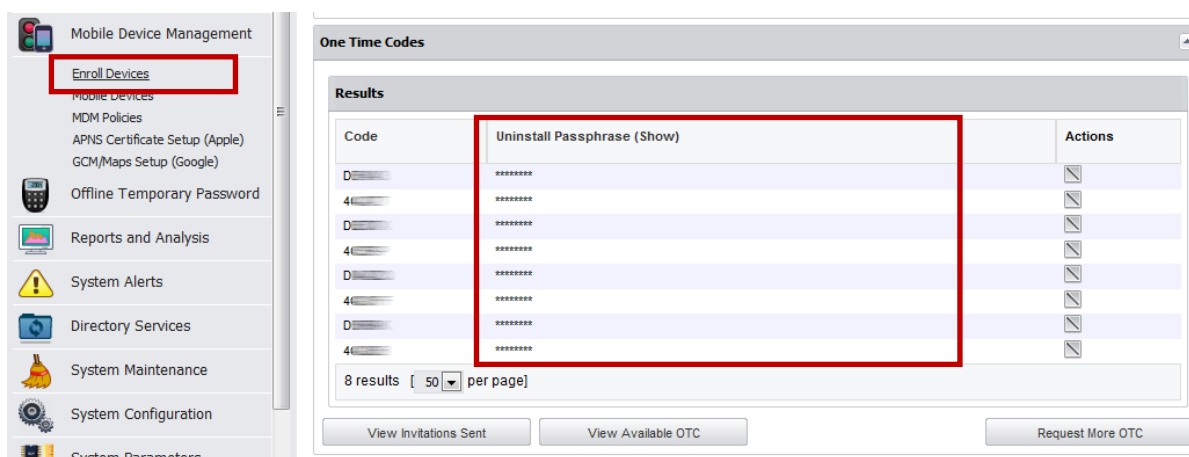
A practical example to illustrate this fact better is the following. An iPhone is enrolled and the administrator applies the companies' security policy for restrictions (disabling FaceTime for example) and WiFi Settings as a profile and protects it with a profile protection. The user of the device wants 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 WiFi 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 devices 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 screenshot displays the Endpoint Protector web interface. On the left sidebar, the 'Mobile Device Management' section is expanded, and 'Enroll Devices' is highlighted. The main content area is titled 'One Time Codes'. Below this, a 'Results' section contains a table with three columns: 'Code', 'Uninstall Passphrase (Show)', and 'Actions'. The 'Uninstall Passphrase (Show)' column is highlighted with a red box and contains a list of passphrases. Below the table, there are buttons for 'View Invitations Sent', 'View Available OTC', and 'Request More OTC'.

Code	Uninstall Passphrase (Show)	Actions
D	*****	
4	*****	
D	*****	
4	*****	
D	*****	
4	*****	
D	*****	
4	*****	

8 results [ 50 per page]

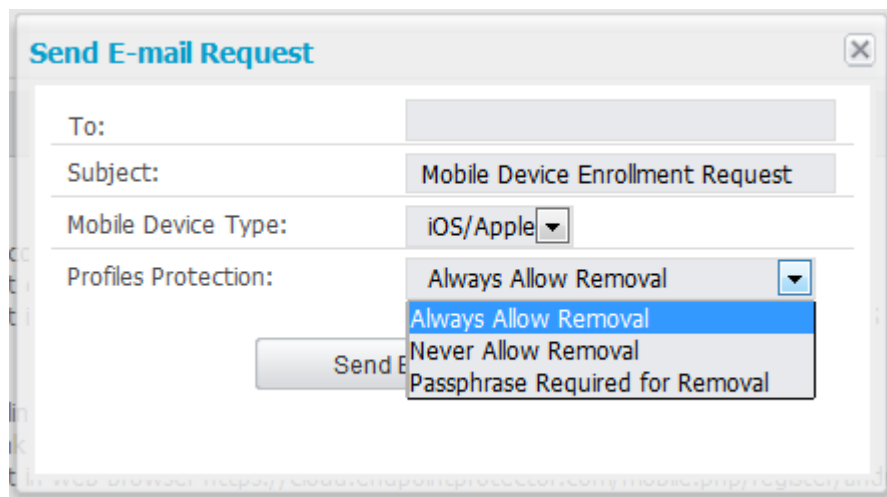
[View Invitations Sent](#) [View Available OTC](#) [Request More OTC](#)

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

The screenshot displays the Endpoint Protector Mobile Device Management interface. On the left is a sidebar menu with the following items: Mobile Device Management (selected), Enroll Devices, Mobile Devices (highlighted with a red box), MDM Policies, APNS Certificate Setup (Apple), GCM/Maps Setup (Google), Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Locate Mobile Device' and shows 'Current Location' with details: Time: 22 Oct 2012 10:34:35, Provider: N/A, and 'Calculating...'. Below this, 'Previous Location' is also shown as 'Calculating... / Unknown'. At the bottom of the main area is a tabbed interface with 'Security Policy', 'Lock / Wipe', 'Device Settings', 'Manage Device' (selected), and 'M...'. The 'Manage Device' tab contains a 'Profile Removal Policy' section (highlighted with a red box) with the following settings: 'Always Allow Removal' (radio button), 'Never Allow Removal' (radio button), 'Passphrase Required for Removal' (radio button, selected), and 'Passphrase' (text field containing 'PASSREMOVE'). A 'Save' button is located below the passphrase field. To the right of the 'Profile Removal Policy' section is a 'Refresh Device I' button and a message 'This feature will up'.

### 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”.



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.

#### **Note!**

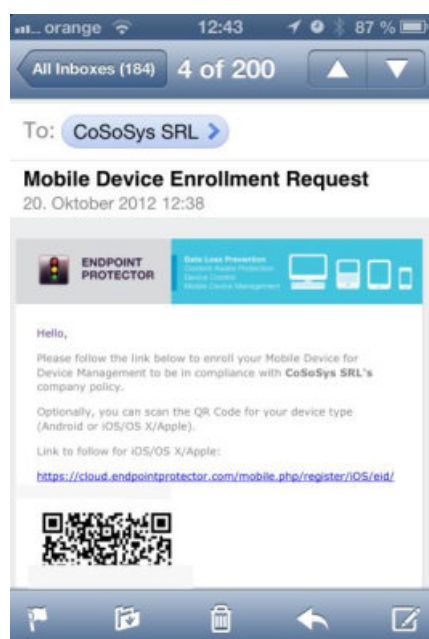
**SMS Enrollment is not available for OS X !**

### 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.



#### **Note!**

SMS Enrollment is not available for OS X!

### 7.2.7. iOS and OS X Mobile Device Enrollment over URL

#### **Attention!**

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.

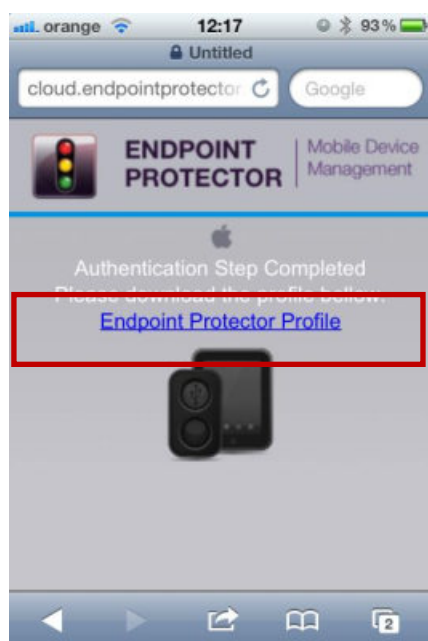
The enrollment of an iOS or OS X device requires a working Internet connection (Wi-Fi or 4G/3G/2G). A 3G data connection is recommended for mobile devices. This way the communication with the Apple Servers can be performed and the information about the mobile device can be further transmitted to the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

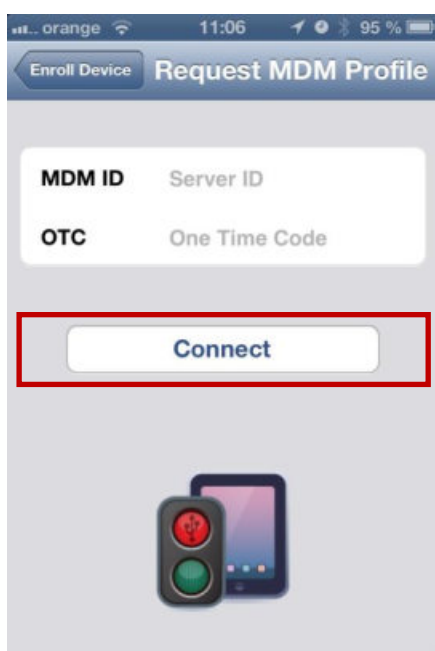


Left image, device not enrolled yet.

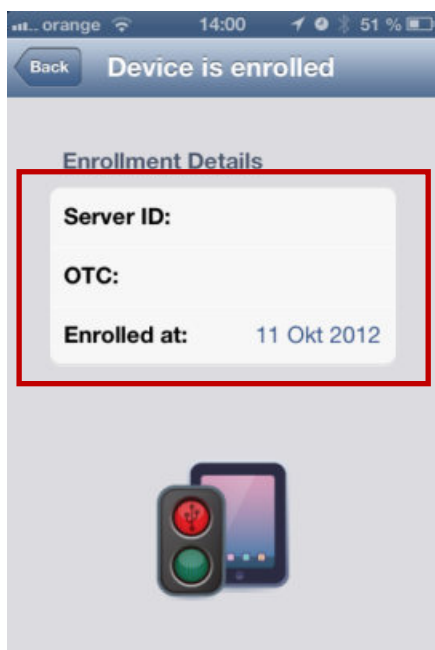


Right image, device is already enrolled.

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

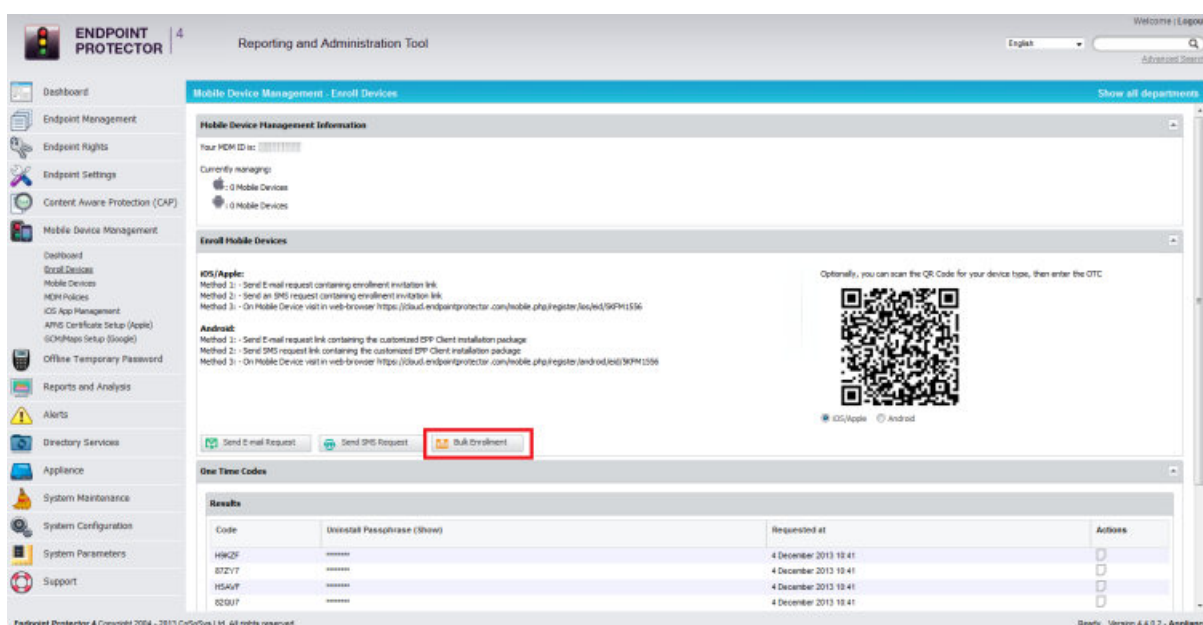
To enroll an Android mobile device, a Google Account is required to be previously setup by the user on the device. This is usually done when the user receives a new device and starts using it. Additionally, an Internet connection is mandatory for the communication between Endpoint Protector Appliance 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.



The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The left sidebar contains navigation links for Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content-Aware Protection (CAP), Mobile Device Management, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Mobile Device Management - Enroll Devices' and includes a 'Show all departments' link. The 'Mobile Device Management Information' section shows the MDM ID and current management status. The 'Enroll Mobile Devices' section provides instructions for iOS/Apple and Android devices, including a QR code for scanning. Below the instructions, there are three buttons: 'Send E-mail Request', 'Send SMS Request', and 'Bulk Enrollment', with the latter being highlighted by a red rectangle. The 'One Time Codes' section displays a table of codes and their request times.

Code	One-time Passphrase (Show)	Requested at	Actions
H9K2F	*****	4 December 2013 13:41	[icon]
STZV7	*****	4 December 2013 13:41	[icon]
HS4VF	*****	4 December 2013 13:41	[icon]
SDUJ7	*****	4 December 2013 13:41	[icon]

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

Import contacts list

Select Mobile Device Type:

☒ iOS/Apple
 ☐ Android
 ☐ Unknown

Profiles Protection:

☒ Always Allow Removal
 ☐ Never Allow Removal
 ☐ Passphrase Required for Removal

Browse for the import file:

No file selected.

Download sample file:

[Bulk Enrollment .xls Sample](#)

Upload

---

Paste Contacts

Select Mobile Device Type:

☒ iOS/Apple
 ☐ Android
 ☐ Unknown

Profiles Protection:

☒ Always Allow Removal
 ☐ Never Allow Removal
 ☐ Passphrase Required for Removal

Contacts List:

Maximum 500 contacts at once.

Example:

Admin,admin@example.com,+4975419782627  
 John Doe; john@company.com; 004975419782627  
 Mark; mark@internal  
 Jane Doe; ;4975419782627

Save

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](mailto: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.

List of Mobile Device Management Bulk Enrollment Contacts Show all departments

**Important Notice**

- Please select the Mobile Device Type and Default Profiles Protection Type when importing/pasting contacts since the Enrollment Requests will contain these information;
- If the contact contains both an E-mail address and a phone number, the request will be sent to the E-mail address;
- Sending Enrollment Requests to the maximum accepted entries in the sending queue will take up to 1 hour, depending on the number of selected contacts.

**Results**

<input type="checkbox"/> 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	

4 results [ 20 per page]

Add To Sending Queue Delete Contacts

**Import contacts list**

Select Mobile Device Type: ☒ iOS/Apple ☐ Android ☐ Unknown

Profiles Protection: ☒ Always Allow Removal ☐ Never Allow Removal ☐ Passphrase Required for Removal

Browse for the import file:  No file selected.

Download sample file: [Bulk Enrollment .xls Sample](#)

Upload

**Paste Contacts**

Select Mobile Device Type: ☒ iOS/Apple ☐ Android ☐ Unknown

Profiles Protection: ☒ Always Allow Removal ☐ Never Allow Removal ☐ Passphrase Required for Removal

Contacts List:

Maximum 500 contacts at once.

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

List of Mobile Device Management Bulk Enrollment Contacts Show all departments

**Important Notice**

- Please select the Mobile Device Type and Default Profiles Protection Type when importing/pasting contacts since the Enrollment Requests will contain these information;
- If the contact contains both an E-mail address and a phone number, the request will be sent to the E-mail address;
- Sending Enrollment Requests to the maximum accepted entries in the sending queue will take up to 1 hour, depending on the number of selected contacts.

**Results**

<input type="checkbox"/> All	Type	Contact	E-mail	Phone	Actions
<input checked="" type="checkbox"/>	iOS	John A.	john@company.com	074xxxxxxx	
<input checked="" 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	

4 results [ 20 per page]

Add To Sending Queue Delete Contacts

**Import contacts list**

Select Mobile Device Type: ☒ iOS/Apple ☐ Android ☐ Unknown

Profiles Protection: ☒ Always Allow Removal ☐ Never Allow Removal ☐ Passphrase Required for Removal

Browse for the import file:  No file selected.

Download sample file: [Bulk Enrollment .xls Sample](#)

Upload

**Paste Contacts**

Select Mobile Device Type: ☒ iOS/Apple ☐ Android ☐ Unknown

Profiles Protection: ☒ Always Allow Removal ☐ Never Allow Removal ☐ Passphrase Required for Removal

Contacts List:

Maximum 500 contacts at once.

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.

List of Mobile Device Management Bulk Enrollment ContactsShow all departments

Added selected contacts (2 in total) to the Sending Queue.

Current Sending Queue contains 2 entries (maximum is 50) [Check Sending Queue](#)

Important Notice

Please select the Mobile Device Type and Default Profiles Protection Type when importing/pasting contacts since the Enrollment Requests will contain these information;

If the contact contains both an E-mail address and a phone number, the request will be sent to the E-mail address;

Sending Enrollment Requests to the maximum accepted entries in the sending queue will take up to 1 hour, depending on the number of selected contacts.




Results

AllType ^ContactE-mailPhoneActions

Paul C

paul@example.com




074xxxxxxx



Dan D

dan@example.com

074xxxxxxx



2 results [ 20 per page]

Add To Sending Queue

Delete Contacts

Import contacts list

Select Mobile Device Type:

IOS/Apple

Android

Unknown

Profiles Protection:

Always Allow Removal

Never Allow Removal

Password Required for Removal

Browse for the import file:

Browse...

No file selected.

Download sample file:

Bulk Enrollment .xls Sample

Upload

Paste Contacts

IOS/AppleAndroidUnknown

## 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.

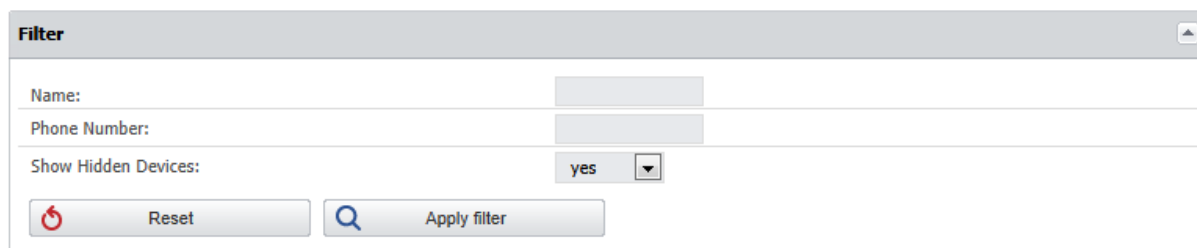
To manage a specific device, select it from the list by right-clicking on the device name and choose one of the available actions: **Manage Device (edit)**, **Hide**, **Show** and **Delete**.



*Manage Device, Hide, Delete*

The **Manage Device** option allows the Administrator to separately manage an already enrolled device and enforce different settings to the device such as security settings specifically for the selected device.

The **Hide** option once selected will remove the mobile device from the list without deleting the mobile device history or uninstalling / unmanaging the device. A hidden device can be added again to the list of mobile devices by selecting the “Show Hidden Devices” > Yes > “Apply Filter” option from the available Filter option.



The screenshot shows a 'Filter' dialog box with a title bar. Inside, there are three input fields: 'Name:', 'Phone Number:', and 'Show Hidden Devices:'. The 'Show Hidden Devices:' field has a dropdown menu currently set to 'yes'. At the bottom, there are two buttons: 'Reset' (with a circular arrow icon) and 'Apply filter' (with a magnifying glass icon).













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.

### Note!

We recommend using the “Hide” option instead of deleting the mobile device in order to keep the mobile device history for later auditing.

## 8.1. Mobile Device Status

Mobile Devices >

Filter											
Results											
Type	Name	Description	Ownership	Username	Model	Carrier	Phone Number	OS Version	Status	Last Seen	Actions
	iPhone		unknown		iPhone3,1 MC603RR			5.1.1	MobileProfileRemoved	20 October 2012 11:57	 
	Samsung GT-I9100		unknown		Samsung GT-I9100			4.0.3	Registered	20 October 2012 8:51	 
	Pad 1		unknown		IPad1,1 MB292LL			5.0.1	Registered	19 October 2012 17:45	 
	iPhone		company		iPhone3,1 MC603RR			6.0	Registered	19 October 2012 17:38	 
4 results [ 50 per page]											

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

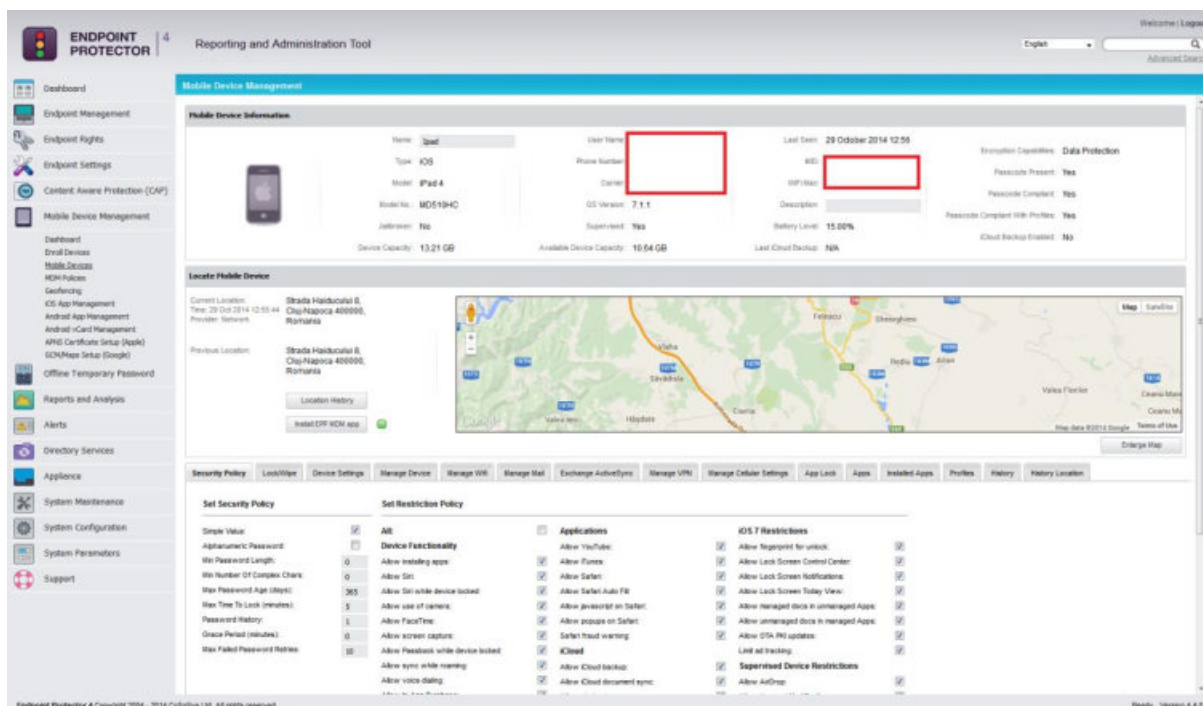
**Registered** – means the device is currently managed and Endpoint Protector MDM can communicate with the device. Applies to both iOS and Android devices.

**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 (ie. Differences apply between iOS and Android)
- **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.

For each of the available Mobile Device Management options a status bullet is displayed indicating the returned result of a selected/executed operation:

-  Red indicates that the requested operation has failed.
-  Green indicates that the requested operation was successfully performed.
-  Yellow indicates that the requested operation is in pending mode.





























A practical example is when you click on “Refresh Device Details”. The bullet will turn yellow and stay for a few seconds in the yellow color until the request has been sent to the device and the device has answered to the Endpoint Protector Appliance. Then the status is changed to green and in this case the updated device details can be viewed.

**Note!**

Due to the differences existing between the iOS, OS X and Android platforms, some of the MDM features might not be available for all the operating systems.

### 8.1.1. 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	FileVault 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 password 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	 /  / 

Security Policy	Password History	Keeps a track of the last passwords used and doesn't allow setting them as new passwords	
Security Policy	Password Age	Enforces the user to define a new password after a certain time period	 / 
Security Policy	Grace Period	Enforces the user to define a new password after the grace period is over (counted in minutes)	 / 
Manage Device	Play Sound on Device	Activates a song on the device, which will play for a predefined period of time	
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	 /  / 

# 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.

**Security Policy** | Lock/Wipe | Device Settings | Manage Device | Manage Wifi | Manage Mail | Manage VPN | Manage Cellular Settings | Apps | Installed Apps | Profiles | History

---

**Set Security Policy** | **Clear Password (No more password required)** | **Set Restriction Policy**

**Set Security Policy**

Simple Value: ☐ This feature will reset the current device password to be empty; hence the device can be unlocked without entering a password.

Alphanumeric Password: ☐

Min Password Length:

Min Number Of Complex Chars:

Max Password Age (days):

Max Time To Lock (minutes):

Password History:

Grace Period (minutes):

Max Failed Password Retries:

**Clear Password (No more password required)**

**Set Restriction Policy**

**All:**

**Device Functionality**

Allow installing apps: ☒

Allow Siri: ☒

Allow Siri while device locked: ☒

Allow use of camera: ☒

Allow FaceTime: ☒

Allow screen capture: ☒

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: ☒

**Applications**

Allow YouTube: ☒

Allow iTunes: ☒

Allow Safari: ☒

Allow Safari Auto Fill: ☒

Allow javascript on Safari: ☒

Allow popups on Safari: ☒

Safari fraud warning: ☒

**iCloud**

Allow iCloud backup: ☒

Allow iCloud document sync: ☒

Allow photo stream: ☒

Allow shared photo streams: ☒

**Security and Privacy**

Allow sending diagnostic data: ☒

Allow untrusted TLS certificate: ☒

Force encrypted backups: ☒

**Content Rating**

Allow explicit content: ☒

**iOS 7 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: ☒

**Set Settings** ☒ **Clear Password** ☒ **Set Settings** ☒



### 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. 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.

**Set Restriction Policy**

<b>All:</b> <b>Device Functionality</b> Allow installing apps: <input checked="" type="checkbox"/> Allow Siri: <input checked="" type="checkbox"/> Allow Siri while device locked: <input checked="" type="checkbox"/> Allow use of camera: <input checked="" type="checkbox"/> Allow FaceTime: <input type="checkbox"/> Allow screen capture: <input checked="" type="checkbox"/> Allow Passbook while device locked: <input checked="" type="checkbox"/> Allow sync while roaming: <input checked="" type="checkbox"/> Allow voice dialing: <input checked="" type="checkbox"/> Allow In-App Purchase: <input checked="" type="checkbox"/> Require iTunes Store password: <input checked="" type="checkbox"/> Allow multiplayer gaming: <input checked="" type="checkbox"/> Allow adding Game Center friends: <input checked="" type="checkbox"/>	<b>Applications</b> Allow YouTube: <input checked="" type="checkbox"/> Allow iTunes: <input checked="" type="checkbox"/> Allow Safari: <input checked="" type="checkbox"/> Allow Safari Auto Fill: <input checked="" type="checkbox"/> Allow javascript on Safari: <input checked="" type="checkbox"/> Allow popups on Safari: <input checked="" type="checkbox"/> Safari fraud warning: <input checked="" type="checkbox"/> <b>iCloud</b> Allow iCloud backup: <input checked="" type="checkbox"/> Allow iCloud document sync: <input checked="" type="checkbox"/> Allow photo stream: <input checked="" type="checkbox"/> Allow shared photo streams: <input checked="" type="checkbox"/> <b>Security and Privacy</b> Allow sending diagnostic data: <input checked="" type="checkbox"/> Allow untrusted TLS certificate: <input checked="" type="checkbox"/> Force encrypted backups: <input checked="" type="checkbox"/> <b>Content Rating</b> Allow explicit content: <input checked="" type="checkbox"/>	<b>iOS7 Restrictions</b> Allow fingerprint for unlock: <input checked="" type="checkbox"/> Allow Control Center on Lock Screen: <input checked="" type="checkbox"/> Allow Lock Screen Notifications: <input checked="" type="checkbox"/> Allow Lock Screen Today View: <input checked="" type="checkbox"/> Allow managed docs in unmanaged Apps: <input checked="" type="checkbox"/> Allow unmanaged docs in managed Apps: <input checked="" type="checkbox"/> Allow OTA PKI updates: <input checked="" type="checkbox"/> Limit ad tracking: <input checked="" type="checkbox"/> <b>Supervised Devices Restrictions</b> Allow AirDrop: <input checked="" type="checkbox"/> Allow Account Modification: <input checked="" type="checkbox"/> Allow App Cellular Data Changes: <input checked="" type="checkbox"/> Allow user generated Siri content: <input checked="" type="checkbox"/> Allow changes to Find My Friends: <input checked="" type="checkbox"/> Allow Host Pairing: <input checked="" type="checkbox"/> Allow iBookstore: <input checked="" type="checkbox"/> Allow Game center: <input checked="" type="checkbox"/> Allow iMessage: <input checked="" type="checkbox"/> Allow App Removal: <input checked="" type="checkbox"/>	<b>iOS8 Restrictions</b> Allow Handoff: <input checked="" type="checkbox"/> Allow managed apps cloud sync: <input checked="" type="checkbox"/> Allow backup of Enterprise books: <input checked="" type="checkbox"/> Allow Enterprise books metadata sync: <input checked="" type="checkbox"/> <b>Supervised Devices Restrictions</b> Allow Erase all Content and Settings: <input checked="" type="checkbox"/> Allow internet results in Spotlight: <input checked="" type="checkbox"/> Allow configuring Restrictions: <input checked="" type="checkbox"/>
---	--	---	--



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. iOS8 Restrictions

- Allow Handoff
- Allow managed apps cloud sync
- Allow backup of Enterprise books
- Allow Enterprise books metadata sync

### 9.2.8. 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/Wipe

Mobile Devices > Lock / Wipe

Lock Device	Clear Password (No more password required)	Wipe Device Data
Lock Device Screen (Keep Current Password) Message: <input type="text" value="test"/> Phone Number: <input type="text" value="1111"/>	This feature will reset the current device password to be empty; hence the device can be unlocked without entering a password.	Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.
<input type="button" value="Lock"/> 	<input type="button" value="Clear Password"/> 	<input type="button" value="Wipe"/> 

### 9.3.1. Lock Device

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.

On Supervised iOS 7 devices it is possible to show a message and a phone number when locking the screen. For the message and phone number to appear the device must have a previously set password.

### 9.3.2. Clear Passcode

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.

### 9.3.3. Remote iOS Device Wipe (Device Nuke)

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.

## 9.4. 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.

## 9.5. Device Ownership

Mobile Devices > Device Settings > Device Ownership

Security Policy Lock / Wipe **Device Settings**

**Device Ownership**

Unknown: ☒

Personal: ☐

Company: ☐

Save

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”.

## 9.6. Voice Roaming on iOS

Mobile Devices > Device Settings > Voice Roaming

Security Policy Lock / Wipe **Device Settings** Manage Device Manage WiFi Manage Mail Ins

**Device Ownership**

Unknown: ☒

Personal: ☐

Company: ☐

Save

**Voice Roaming**

This feature will enable/disable voice roaming on the mobile device.  
Note: This option is carrier dependent, meaning that the carrier has to make the change of this setting.

Enable/Disable: ☐

Apply

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.

## 9.7. Data Roaming on iOS

Mobile Devices > Device Settings > Data Roaming

The screenshot shows the 'Device Settings' tab in the Endpoint Protector MDM interface. The 'Data Roaming' section is highlighted with a red box. It contains the following text: 'This feature will enable/disable data roaming on the mobile device.' Below this is an 'Enable/Disable' toggle switch, which is currently turned off. At the bottom right of the section is an 'Apply' button.

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

The screenshot shows the 'Manage Device' tab in the Endpoint Protector MDM interface. The 'Profile Removal Policy' section is highlighted with a red box. It contains the following text: 'Always Allow Removal:' with a selected radio button, 'Never Allow Removal:' with an unselected radio button, and 'Passphrase Required for Removal:' with an unselected radio button. Below these is a 'Passphrase:' field with the text 'YE8QXHG6'. At the bottom right of the section is a 'Save' button.

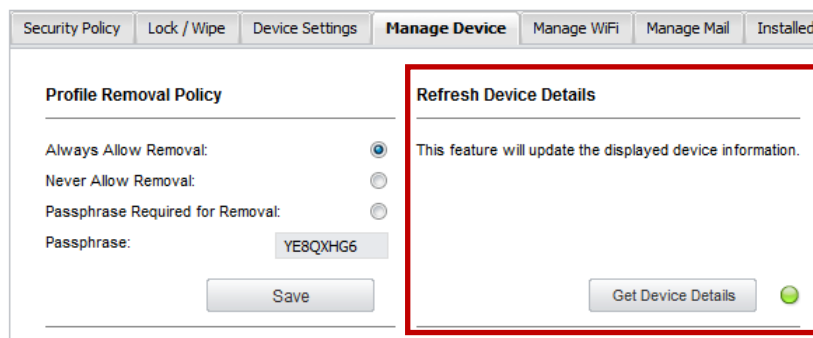
As described in the chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase before the profiles (settings) on an iOS Device can be protected with a passphrase. In this option the passphrase can be changed to be a different one than the one automatically generated and associated with the OTC.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



description of this option please consult chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase.

## 9.9. Refresh Device Details for iOS

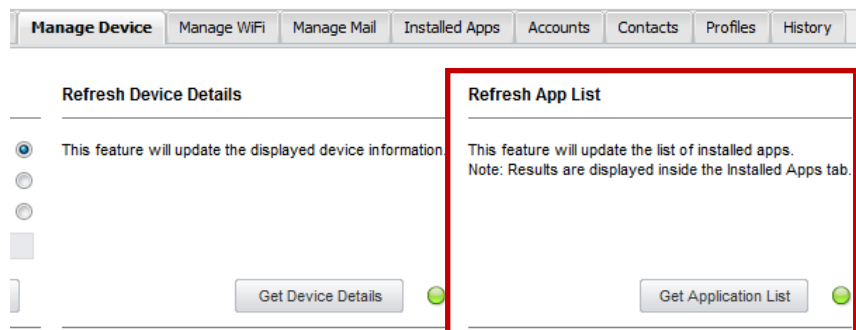
Mobile Devices > Manage Device > Refresh Device Details



This function will ask the iOS devices for its latest details and display them in the Mobile Device Information section.

## 9.10. Refresh App List for iOS

Mobile Devices > Manage Device > Refresh App List



This function by clicking "Get Application List" 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 "Get Application List" button.

## 9.11. 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 9.10 Refresh App List for iOS.

Results								
Name	Identifier	Version	Short Version	Last Status	App Size	Storage Used	Management Flags	Actions
Adobe Reader	com.adobe.Adobe-Reader	73784	10.5.2	Managed	18.81 MB	420 KB	⬆️⬆️	⊗ ⬆️
Angry Birds	com.rovio.angrybirdsfree	1.5.1	1.5.1	Managed	124.62 MB	8 KB	⬆️⬆️	⊗ ⬆️
EPP MDM	com.cososys.EPPMDM	1.0.0.6	0.1	Managed	536 KB	296 KB	⬆️⬆️	⊗ ⬆️
iBooks	com.apple.iBooks	1523	3.1	Managed	53.5 MB	8 KB	N/A	⊗ ⬆️
TED	com.ted.TED	2028	2100	Managed	23.27 MB	8 KB	N/A	⊗ ⬆️

5 results ( 50 per page)

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.

## 9.12. Refresh Profile List on iOS

Mobile Devices > Manage Device > Refresh Profile List

Manage Device	Manage WiFi	Manage Mail	Installed Apps	Accounts	Contacts	Profiles	History
<b>Refresh Device Details</b> This feature will update the displayed device information. Get Device Details		<b>Refresh App List</b> This feature will update the list of installed apps. Note: Results are displayed inside the Installed Apps tab. Get Application List		<b>Refresh Profile List</b> This feature will update the list of installed profiles. Note: Results are displayed inside the Profiles tab. Refresh List			

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.

## 9.13. Profiles on iOS Devices Information


Mobile Devices > Profiles

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

1 result ( 50 per page)

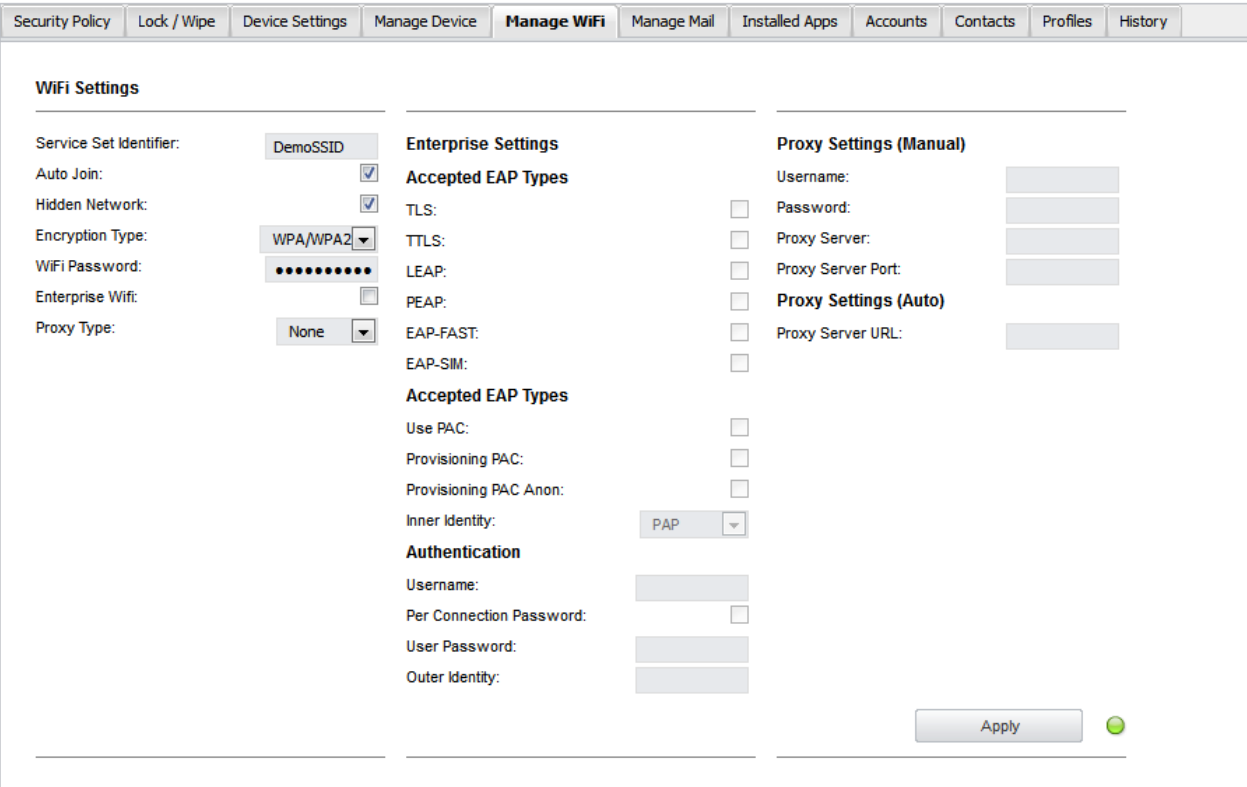
The profiles installed on an iOS Device are listed in the “Profile” tab. The Profiles installed on an iOS Device are always the enrollment Profile and possible restriction or other profiles. The type of profile is shown in the “Profile Description” column.

### 9.13.1. 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.

## 9.14. Manage WiFi on iOS

Mobile Devices > Manage WiFi



The screenshot displays the 'Manage WiFi' configuration page. At the top, there is a navigation bar with tabs: Security Policy, Lock / Wipe, Device Settings, Manage Device, **Manage WiFi**, Manage Mail, Installed Apps, Accounts, Contacts, Profiles, and History. Below the navigation bar, the 'WiFi Settings' section is active. It is divided into three main columns:

- Left Column:**
  - Service Set Identifier: DemoSSID
  - Auto Join: ☒
  - Hidden Network: ☒
  - Encryption Type: WPA/WPA2
  - WiFi Password: [Masked]
  - Enterprise Wifi: ☐
  - Proxy Type: None
- Middle Column:**
  - Enterprise Settings**
  - Accepted EAP Types**
    - TLS: ☐
    - TTLS: ☐
    - LEAP: ☐
    - PEAP: ☐
    - EAP-FAST: ☐
    - EAP-SIM: ☐
  - Accepted EAP Types**
    - Use PAC: ☐
    - Provisioning PAC: ☐
    - Provisioning PAC Anon: ☐
    - Inner Identity: PAP
  - Authentication**
    - Username: [Field]
    - Per Connection Password: ☐
    - User Password: [Field]
    - Outer Identity: [Field]
- Right Column:**
  - Proxy Settings (Manual)**
    - Username: [Field]
    - Password: [Field]
    - Proxy Server: [Field]
    - Proxy Server Port: [Field]
  - Proxy Settings (Auto)**
    - Proxy Server URL: [Field]

At the bottom right of the settings area, there is an 'Apply' button and a green status indicator.

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

### 9.14.1. Wipe Wi-fi Settings

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

## 9.15. Manage Mail on iOS

Mobile Devices > Manage Mail

The screenshot displays the 'Manage Mail' configuration page. At the top, a navigation bar includes tabs for Security Policy, Lock / Wipe, Device Settings, Manage Device, Manage WiFi, **Manage Mail**, Installed Apps, Accounts, Contacts, Profiles, and History. Below the navigation bar, the 'Mail Settings' section is active. It contains three main areas: 'Account Description' on the left, 'Incoming Mail' in the center, and 'Outgoing Mail' on the right. The 'Account Description' section includes fields for Account Type (IMAP), IMAP Path Prefix (imap.company), User Display Name (Demo User), Email Address (emo@company), and Allow Move (checked). The 'Incoming Mail' section includes fields for Mail Server (pop.company.c), Port, Username (demo@company), Auth Type (None), Password (masked with dots), and Use SSL (checked). The 'Outgoing Mail' section includes fields for Mail Server (smtp.company.), Port, Username (emo@company), Auth Type (None), Password (masked with dots), Use SSL (checked), Use incoming password (checked), Disable Address Syncing (unchecked), and Use only in Mail (unchecked). An 'Apply' button and a green status indicator are located at the bottom right of the settings area.

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.

### 9.15.1. 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.

## 9.16. Exchange Active Sync

Mobile Devices > Exchange Active Sync

The screenshot displays the 'Exchange Active Sync' configuration page. At the top, a navigation bar includes tabs for Security Policy, Lock/Wipe, Device Settings, Manage Device, Manage Wifi, Manage Mail, and **Exchange Active Sync**. Below the navigation bar, the 'Exchange ActiveSync Settings' section is active. It contains two main areas: 'General Settings' on the left and 'Domain Settings' on the right. The 'General Settings' section includes fields for Account Name, Exchange Host, Prevent Move (unchecked), Disable Recent Mail Syncing (unchecked), Use only in Mail app (unchecked), and Use SSL (unchecked). The 'Domain Settings' section includes fields for Domain, User, Email Address, Email Password, and Past Days of Mail to Sync. An 'Apply' button and a green status indicator are located at the bottom right of the settings area.

The Endpoint Protector Administrator can apply Exchange Account 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.

## 9.17. Manage VPN on iOS

Mobile Devices > Manage VPN

The screenshot shows the 'Manage VPN' settings page. At the top is a navigation bar with tabs: Security Policy, Lock/Wipe, Device Settings, Manage Device, Manage Wifi, Manage Mail, **Manage VPN**, Apps, Installed Apps, Profiles, and History. Below the navigation bar is the 'VPN Settings' section. It contains several fields: 'Connection Name' (text input with 'Demo VPN'), 'Connection Type' (dropdown menu with 'L2TP'), 'Provider' (dropdown menu with 'Custom'), and 'Proxy Type' (dropdown menu with 'None'). To the right of these are 'Auth type' (dropdown menu with 'Password'), 'Server' (text input), 'Account Name' (text input), 'Password' (text input), 'Route all traffic' (checkbox), and 'Shared Secret' (text input). Further right is the 'Proxy Settings (Manual)' section with 'Username' (text input), 'Password' (text input), 'Proxy Server' (text input), and 'Proxy Server Port' (text input). Below that is the 'Proxy Settings (Auto)' section with 'Proxy Server URL' (text input). At the bottom right is an 'Apply' button and a green status indicator.

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.

## 9.18. 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.

The screenshot shows the 'Manage APN' settings page. At the top is a navigation bar with tabs: Security Policy, Lock/Wipe, Device Settings, Manage Device, Manage Wifi, Manage Mail, Manage VPN, **Manage APN**, Apps, Installed Apps, Profiles, and History. Below the navigation bar is the 'APN Settings' section. It contains several fields: 'Access Point Name' (text input), 'Access Point Username' (text input), 'Access Point Password' (text input), 'Access Point Proxy' (text input), and 'Proxy Server Port' (text input). At the bottom is an 'Apply' button and a green status indicator.

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.

## 9.19. Manage Cellular Settings on Supervised iOS 7 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 shows the 'Manage Cellular Settings' tab selected in the top navigation bar. Below the navigation bar, the 'Cellular Settings' section contains the following fields:

- Configuration Name: [Text input field]
- Authentication Type: [Dropdown menu showing 'None']
- Access Point Username: [Text input field]
- Access Point Password: [Text input field]
- Access Point Proxy: [Text input field]
- Proxy Server Port: [Text input field]

An 'Apply' button is located at the bottom right of the form, next to a green status indicator.

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.

## 9.20. App Lock on Supervised iOS 7 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.

The screenshot shows the 'App Lock' tab selected in the top navigation bar. The interface is divided into three main sections:

- App Lock Payload:**
  - App Identifier: [Dropdown menu showing 'EPP MDM']
  - Set Options: ☐
  - Set User Options: ☐
- App Lock Options:**
  - Disable Touch: ☐
  - Disable Device Rotation: ☐
  - Disable Volume Buttons: ☐
  - Disable Ringer Switch: ☐
  - Disable Sleep/Wake Button: ☐
  - Disable Auto Lock: ☐
  - Enable VoiceOver: ☐
  - Enable Zoom: ☐
  - Enable Invert Colors: ☐
  - Enable Assistive Touch: ☐
  - Enable Speak Selection: ☐
  - Enable Mono Audio: ☐
- App Lock User Options:**
  - Allow VoiceOver adjustments: ☐
  - Allow Zoom adjustments: ☐
  - Allow Invert Colors adjustments: ☐
  - Allow Assistive Touch adjustments: ☐

An 'Apply' button is located at the bottom right of the form, next to a green status indicator.

If the list of existing applications on the device was never updated on the server, it is a must to press the "Get App List" 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 "Get App List" 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 App Lock on the device.

## 9.21. Installed Apps

## Mobile Devices &gt; Installed Apps

A list of applications already installed on an iOS device can be seen in the “Installed Apps” tab. The list includes apps pushed through Endpoint Protector as well as apps installed directly from the mobile device.

[illegible]































## 9.22. History of iOS Devices Actions

## Mobile Devices &gt; 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.

Security Policy	Lock / Wipe	Device Settings	Manage Device	Manage WiFi	Manage Mail	Installed Apps	Accounts	Contacts	Profiles	History
-----------------	-------------	-----------------	---------------	-------------	-------------	----------------	----------	----------	----------	---------

Results				
Mobile Device	Action	Status	Result Message	Event Time ▾
 iPhone	WifiSettings		Error	19 October 2012 16:58
 iPhone	VoiceRoaming		CommandFormatError	19 October 2012 16:35
 iPhone	MailSettings		Executed	19 October 2012 16:34
 iPhone	VoiceRoaming		CommandFormatError	19 October 2012 16:32
 iPhone	WifiSettings		Executed	19 October 2012 16:31
 iPhone	ClearPasscode		Executed	19 October 2012 16:30
 iPhone	GetInstalledPackages		Executed	19 October 2012 16:30
 iPhone	ProfileList		Executed	19 October 2012 16:30
 iPhone	VoiceRoaming		CommandFormatError	19 October 2012 16:30
 iPhone	MailSettings		Error	19 October 2012 16:30
 iPhone	WifiSettings		Executed	19 October 2012 16:28
 iPhone	MailSettings		Error	19 October 2012 16:28
 iPhone	WifiSettings		Error	19 October 2012 16:28
 iPhone	GetDeviceInfo		Executed	19 October 2012 16:26
 iPhone	GetDeviceInfo		Executed	19 October 2012 16:24

15 results [ 50 ▾ ] per page

## 9.23. History Location

Mobile Devices &gt; History Location

The “History Location” tab shows a list of the last ten locations of the iOS device. Although these locations are also displayed in other tabs, this list provides a faster and a better overview.

[illegible]



# 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 OS X Management console interface. At the top, there is a navigation bar with tabs: Security Policy, Lock/Wipe, Device Settings, Manage Device, Manage Wifi, Manage Mail, Manage VPN, Installed Apps, Profiles, and History. The 'Security Policy' tab is selected. Below the navigation bar, the 'Set Password Security Policy' section is highlighted with a red box. This section contains the following settings:

- Simple Value: ☒
- Alphanumeric Password: ☐
- Min Password Length: 0
- Min Number Of Complex Chars: 0
- Max Password Age (days): 365
- Max Time To Lock (minutes): 5
- Password History: 1
- Grace Period (minutes): 0

At the bottom of this section is a 'Set Settings' button with a green status indicator.

To the right of the highlighted section, there are two other sections:

- FileVault 2 Disk Encryption:** Contains settings for File Vault (set to 'Off / Disable'), Defer Encryption, Prompt user for missing info, Create a personal recovery key, Display the recovery key to the user, Use KeyChain for institutional recovery key, Output Path, Username, and Password. A notice states: 'Notice: This operation can take a long time to complete'. There is a 'Set Settings' button with a green status indicator.
- Disk Encryption Status:** A table showing the status of encryption:

Disk Encryption Status	
Encryption Status:	Disabled
Personal Recovery Key:	Not Defined
Institutional Recovery Key:	Not Defined

At the bottom of this section is a 'Refresh' button with a green status indicator.

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

**Set Password Security Policy**

Simple Value: ☒

Alphanumeric Password: ☐

Min Password Length:

Min Number Of Complex Chars:

Max Password Age (days):

Max Time To Lock (minutes):

Password History:

Grace Period (minutes):

**FileVault 2 Disk Encryption**

File Vault:

Defer Encryption: ☐

Prompt user for missing info: ☐

Create a personal recovery key: ☐

Display the recovery key to the user: ☐

Use KeyChain for institutional recovery key: ☐

Output Path:

Username:

Password:

Notice: This operation can take a long time to complete

**Disk Encryption Status**

Encryption Status: Disabled

Personal Recovery Key: Not Defined

Institutional Recovery Key: Not Defined

Here are some guidelines on how to use the FileVault 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** - FileVault 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 FileVault 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

FileVault 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

**Lock Device**

Lock Device Screen

Lock PIN:

Lock ●

**Wipe Device Data**

Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.

Wipe ●

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

**Lock Device**

Lock Device Screen

Lock PIN:

Lock ●

**Wipe Device Data**

Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.

Find My Mac PIN:

Wipe ●

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.

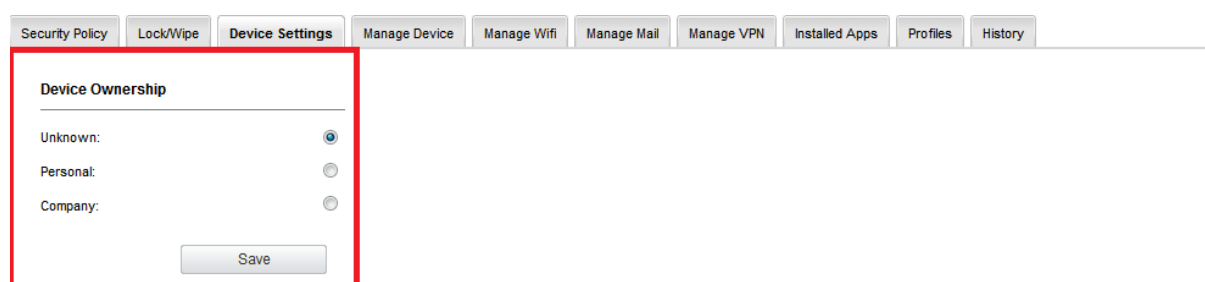
The “Find My Mac PIN” password protects the wiped device. After the device is wiped it will be locked and cannot be used unless the PIN is entered.

### 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

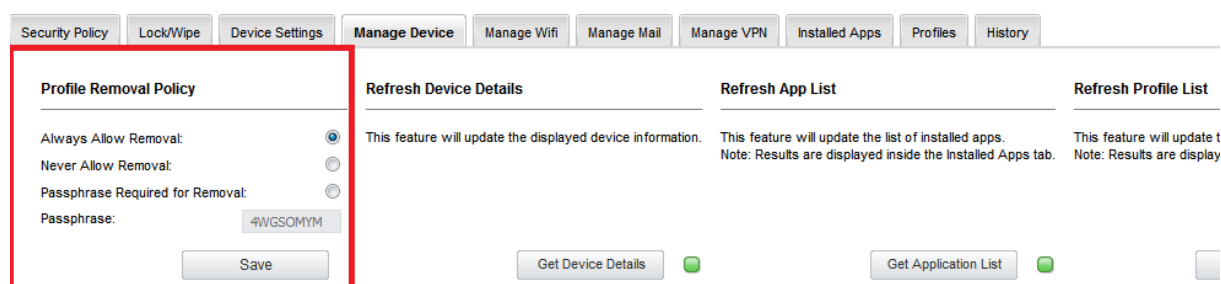


The screenshot shows the 'Device Ownership' settings page. The 'Device Ownership' tab is selected. The 'Unknown' radio button is selected. The 'Personal' and 'Company' radio buttons are unselected. A 'Save' button is at the bottom.

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 > Manage Device > Profile Removal Policy



The screenshot shows the 'Profile Removal Policy' settings page. The 'Profile Removal Policy' tab is selected. The 'Always Allow Removal' radio button is selected. The 'Never Allow Removal' radio button is unselected. The 'Passphrase Required for Removal' radio button is unselected. The 'Passphrase' field contains '4WGSOMYM'. There are 'Get Device Details', 'Get Application List', and 'Refresh Profile List' buttons.

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 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.

## 10.7. Refresh Device Details for OS X

Mobile Devices > Manage Device > Refresh Device Details

The screenshot shows the 'Manage Device' tab selected in the top navigation bar. Below it, the 'Refresh Device Details' section is highlighted with a red box. This section contains the text 'This feature will update the displayed device information.' and a 'Get Device Details' button with a green status indicator. To the left of this section is the 'Profile Removal Policy' section, and to the right are the 'Refresh App List' and 'Refresh Profile List' sections.

This function will ask the OS X devices for its latest details and display them in the Mobile Device Information section.

## 10.8. Refresh App List for OS X

Mobile Devices > Manage Device > Refresh App List

The screenshot shows the 'Manage Device' tab selected in the top navigation bar. Below it, the 'Refresh App List' section is highlighted with a red box. This section contains the text 'This feature will update the list of installed apps. Note: Results are displayed inside the Installed Apps tab.' and a 'Get Application List' button with a green status indicator. To the left of this section is the 'Refresh Device Details' section, and to the right is the 'Refresh Profile List' section.

This function by clicking "Get Application List" 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 "Get Application List" button.

## 10.9. Installed Apps on OS X

Mobile Devices > Installed 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 "Get Application List" as described in chapter 10.8 Refresh App List for iOS X.

Security Policy   Lock/Wipe   Device Settings   Manage Device   Manage Wifi   Manage Mail   Manage VPN   Installed Apps   Profiles   History								
Results								
Name	Identifier	Version	Short Version	Last Status	App Size	Storage Used	Management Flags	Actions
SonPianteServer	com.apple.SonPianteServer	1.1.0	1.1.0	App List Update	2.58 MB	N/A	N/A	
ADAssessantService	com.apple.ADAssessantService	8.0	8.0	App List Update	51.72 KB	N/A	N/A	
Activity Monitor	com.apple.ActivityMonitor	10.9.0	10.9.0	App List Update	10.88 MB	N/A	N/A	
AddressBookManager	com.apple.AddressBookManager	8.0	8.0	App List Update	32.63 KB	N/A	N/A	
AddressBookSourceSync	com.apple.AddressBookSourceSync	8.0	8.0	App List Update	51.78 KB	N/A	N/A	
AddressBookUIForwarder	com.apple.AddressBookUIForwarder	8.0	8.0	App List Update	251.5 KB	N/A	N/A	
AirPlayUIAgent	com.apple.AirPlayUIAgent	2.0	2.0	App List Update	55.47 KB	N/A	N/A	
AirPort Base Station Agent	com.apple.AirPortBaseStationAgent	2.2	2.2	App List Update	130.15 KB	N/A	N/A	
AirPort Utility	com.apple.airport.airportutility	6.3.2	6.3.2	App List Update	48.11 MB	N/A	N/A	

## 10.10. Refresh Profile List on OS X



Mobile Devices > Manage Device > Refresh Profile List

Security Policy   Lock/Wipe   Device Settings   Manage Device   Manage Wifi   Manage Mail   Manage VPN   Installed Apps   Profiles   History			
<b>Profile Removal Policy</b> Always Allow Removal: <input checked="" type="radio"/> Never Allow Removal: <input type="radio"/> Passphrase Required for Removal: <input type="radio"/> Passphrase: <input type="text" value="4WGSOMYM"/> <input type="button" value="Save"/>	<b>Refresh Device Details</b> This feature will update the displayed device information. <input type="button" value="Get Device Details"/>	<b>Refresh App List</b> This feature will update the list of installed apps. Note: Results are displayed inside the Installed Apps tab. <input type="button" value="Get Application List"/>	<b>Refresh Profile List</b> This feature will update the list of installed profiles. Note: Results are displayed inside the Profiles tab. <input type="button" value="Refresh List"/>

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.


## 10.11. Profiles on OS X Devices Information

Mobile Devices > Profiles

Security Policy   Lock/Wipe   Device Settings   Manage Device   Manage Wifi   Manage Mail   Manage VPN   Installed Apps   Profiles   History			
Results			
Profile Name	Profile Description	Profile Identifier	Actions
Endpoint Protector	Endpoint Protector Enrollment Profile	com.endpointprotector.cloud	 

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.

### 10.11.1. 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.

## 10.12. Manage WiFi on OS X

Mobile Devices > Manage WiFi

The screenshot displays the 'Manage WiFi' configuration page. At the top, there is a navigation bar with tabs: Security Policy, Lock/Wipe, Device Settings, Manage Device, **Manage Wifi**, Manage Mail, Manage VPN, Installed Apps, Profiles, and History. Below the navigation bar, the 'WiFi Settings' section is active. It contains several configuration areas:

- Service Set Identifier:** A dropdown menu set to 'Demo'.
- Auto Join:** A checkbox that is checked.
- Hidden Network:** A checkbox that is checked.
- Encryption Type:** A dropdown menu set to 'WPA/WPA2'.
- WiFi Password:** A text field with masked characters (dots).
- Enterprise Wifi:** A checkbox that is unchecked.
- Proxy Type:** A dropdown menu set to 'None'.
- Enterprise Settings:**
  - Accepted EAP Types:**
    - TLS: ☐
    - TTLS: ☐
    - LEAP: ☐
    - PEAP: ☐
    - EAP-FAST: ☐
    - EAP-SIM: ☐
  - EAP-FAST:**
    - Use PAC: ☐
    - Provisioning PAC: ☐
    - Provisioning PAC Anon: ☐
    - Inner Identity: A dropdown menu set to 'PAP'.
  - Authentication:**
    - Username: A text field.
    - Per Connection Password: ☐
    - User Password: A text field.
    - Outer Identity: A text field.
- Proxy Settings (Manual):**
  - Username: A text field.
  - Password: A text field.
  - Proxy Server: A text field.
  - Proxy Server Port: A text field.
  - Proxy Settings (Auto):**
    - Proxy Server URL (PAC): A text field.

At the bottom right of the configuration area, there is an 'Apply' button and a green status indicator.

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

### 10.12.1. Wipe Wi-fi Settings

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

## 10.13. Manage Mail on OS X

Mobile Devices > Manage Mail



Security Policy	Lock/Wipe	Device Settings	Manage Device	Manage Wifi	<b>Manage Mail</b>	Manage VPN	Installed Apps	Profiles	History
-----------------	-----------	-----------------	---------------	-------------	--------------------	------------	----------------	----------	---------

---

### E-mail Settings

Account Description:	Demo User	<b>Incoming Mail</b>	<b>Outgoing Mail</b>
Account Type:	IMAP	E-mail Server:	pop.company.c
IMAP Path Prefix:	imap.company	Port:	
User Display Name:	Demo User	Username:	demo@compan
E-mail Address:	demo@compan	Auth Type:	None
Allow Move:	<input checked="" type="checkbox"/>	Password:	.....
		Use SSL:	<input checked="" type="checkbox"/>
		E-mail Server:	smtp.company.
		Port:	
		Username:	demo@compan
		Auth Type:	None
		Password:	.....
		Use SSL:	<input type="checkbox"/>
		Use incoming settings:	<input type="checkbox"/>
		Use incoming password:	<input checked="" type="checkbox"/>
		Disable Address Syncing:	<input type="checkbox"/>
		Use only in Mail app:	<input type="checkbox"/>
		<input type="button" value="Apply"/> <input checked="" type="checkbox"/>	

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.

### 10.13.1. 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.

## 10.14. Manage VPN on OS X

Mobile Devices > Manage VPN

Security Policy	Lock/Wipe	Device Settings	Manage Device	Manage Wifi	Manage Mail	<b>Manage VPN</b>	Installed Apps	Profiles	History
-----------------	-----------	-----------------	---------------	-------------	-------------	-------------------	----------------	----------	---------

---

### VPN Settings

Connection Name:		Authentication Type:	Password	<b>Proxy Settings (Manual)</b>
Connection Type:	L2TP	Server:		Username:
Provider:	Custom	Account Name:		Password:
Proxy Type:	None	Password:		Proxy Server:
		Route all traffic:	<input type="checkbox"/>	Proxy Server Port:
		Shared Secret:		<b>Proxy Settings (Auto)</b>
				Proxy Server URL:
				<input type="button" value="Apply"/> <input checked="" type="checkbox"/>

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.

## 10.15. 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.

Security Policy	Lock / Wipe	Device Settings	Manage Device	Manage WiFi	Manage Mail	Installed Apps	Accounts	Contacts	Profiles	History
<b>Set Security Policy</b>										
Password Quality:	Alphanumeric	✓								
Min Password Length:	5	✓								
Max Time To Lock (sec):	60	✓								
Max Failed Password Retries:	10	✓								
Ask User to change password:	<input checked="" type="checkbox"/>	✓								
<b>Apply</b>										
<b>Device Password</b>										
Password:										
<b>Set Password</b>										
<b>Current Security Policy</b>										
Password Quality: No requirement										
Min Password Length: 0										
Max Time To Lock (sec): 0										
Max Failed Password Retries: 0										
<b>Refresh</b>										

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

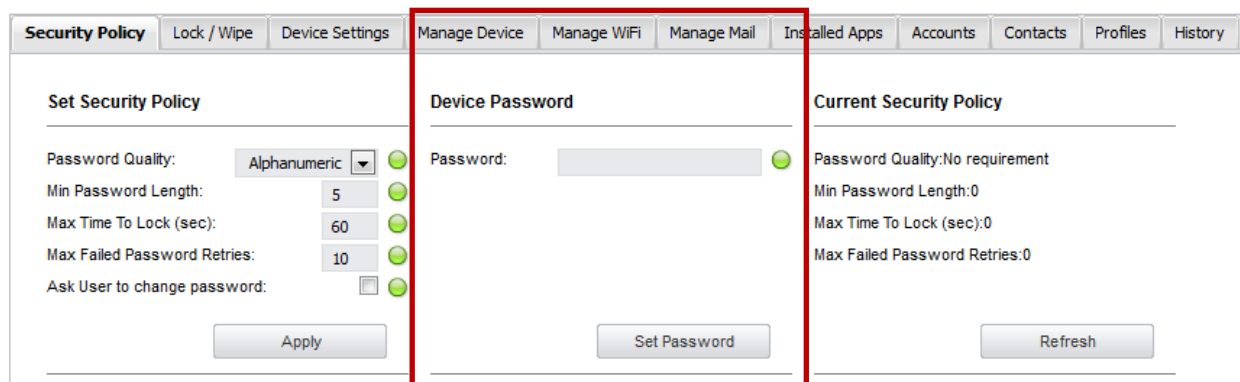
The following Settings can be applied for the password / passcode settings for an Android device:

- **Password Quality** – The following settings can be chosen from:
  - **No requirement**
  - **Any**
  - **Numeric**
  - **Alphabetical**
  - **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 shows the 'Security Policy' management interface. At the top, there is a navigation bar with tabs: 'Security Policy', 'Lock / Wipe', 'Device Settings', 'Manage Device', 'Manage WiFi', 'Manage Mail', 'Installed Apps', 'Accounts', 'Contacts', 'Profiles', and 'History'. Below this, the 'Set Security Policy' section is on the left, containing settings for Password Quality (Alphanumeric), Min Password Length (5), Max Time To Lock (60s), Max Failed Password Retries (10), and a checkbox for 'Ask User to change password'. The 'Device Password' section is highlighted with a red box and contains a 'Password' input field. To the right, the 'Current Security Policy' section shows the current settings, which are currently empty. At the bottom of each section are buttons: 'Apply' for Set Security Policy, 'Set Password' for Device Password, and 'Refresh' for Current Security Policy.

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 Password".

### 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".

The screenshot shows the 'Encrypt Device' section of the mobile device management interface. The 'Request Device Encryption' checkbox is checked, and the 'Enable Encryption' button is visible. The 'Current Security Policy' section on the right shows the status of various security settings.

Set Security Policy	Device Password	Encrypt Device	Current Security Policy
Password Quality: <input type="text" value="No requirement"/> <input checked="" type="checkbox"/> Min Password Length: <input type="text" value="0"/> <input checked="" type="checkbox"/> Max Time To Lock (sec): <input type="text" value="0"/> <input checked="" type="checkbox"/> Max Failed Password Retries: <input type="text" value="0"/> <input checked="" type="checkbox"/> Ask User to change password: <input type="checkbox"/> <input checked="" type="checkbox"/>	Password: <input type="text"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Request Device Encryption	Password Quality: No requirement Min Password Length: 0 Max Time To Lock (sec): 0 Max Failed Password Retries: 0 Device Encryption Request: false Device Encryption Status: ENCRYPTING Wifi Status: Wifi is enabled Bluetooth Status: Bluetooth state

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 screenshot shows the 'Lock Device' section of the mobile device management interface. The 'Lock Device Screen (Keep Current Password)' radio button is selected, and the 'Lock' button is visible.

Security Policy	Lock / Wipe	Device Settings
<b>Lock Device</b> <input type="radio"/> Strong Password Lock (Set Random Password) <input checked="" type="radio"/> Lock Device Screen (Keep Current Password) <input type="button" value="Lock"/> <input checked="" type="checkbox"/>		

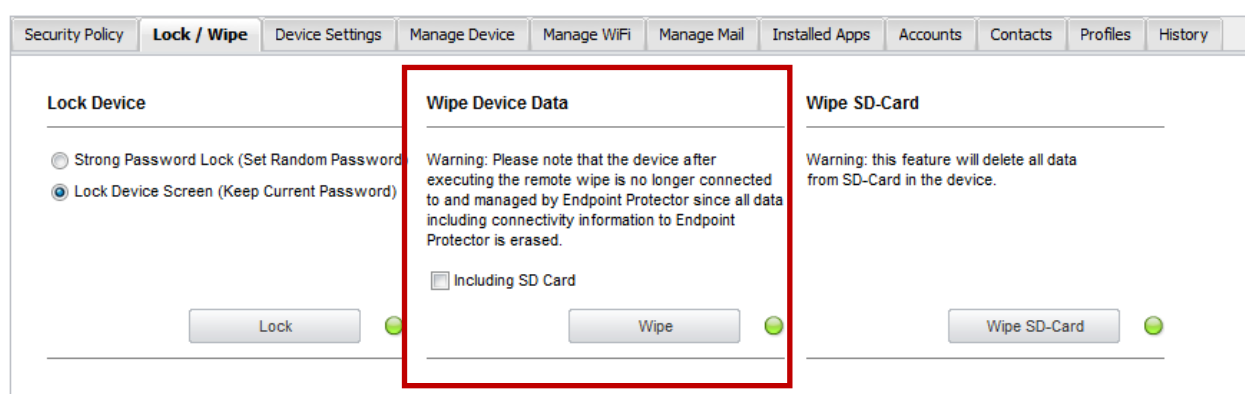
The Android device can be remotely locked. Clicking "Lock" will remotely lock the device screen and require a password entry to unlock the screen.

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.

## 11.4. Remote Android Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data



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.

#### 11.4.1. Android Remote Wipe of SD-Card

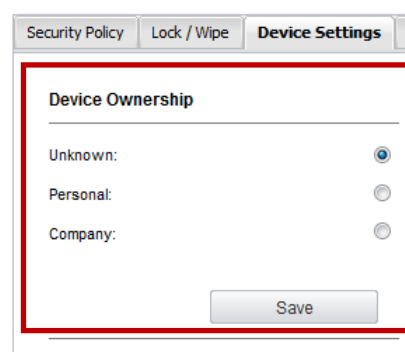
Mobile Devices > Lock / Wipe > Wipe SD-Card



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

## 11.5. Device Ownership

Mobile Devices > Device Settings > Device Ownership



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”.

## 11.6. Android Device Location Settings

Mobile Devices > Device Settings > Device Location Settings



The screenshot shows the 'Device Settings' tab with a sub-tab 'Device Location Settings' highlighted by a red rectangle. On the left, under 'Device Ownership', there are radio buttons for 'Unknown' (selected), 'Personal', and 'Company', with a 'Save' button below. The 'Device Location Settings' section on the right contains two checkboxes, both checked: 'Location Accuracy Fine' and 'Location Cost Allowed'. A 'Save' button is located at the bottom right of this section.

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

### 11.6.1. 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.

### 11.6.2. Location Cost Allowed on Android

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

## 11.7. Manage Wifi

This feature will enable or disable the Wifi on the Android device.

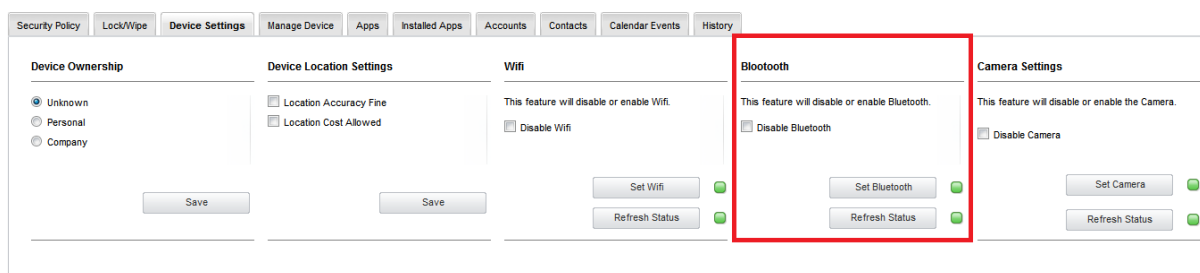
The screenshot shows the 'Device Settings' tab with several sub-tabs. The 'Wifi' sub-tab is highlighted with a red rectangle. It contains the text 'This feature will disable or enable Wifi.' followed by an unchecked checkbox 'Disable Wifi'. Below the checkbox are 'Set Wifi' and 'Refresh Status' buttons, each followed by a green status indicator. To the right, there are sections for 'Bluetooth' and 'Camera Settings' with similar controls and status indicators.

### Note!

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

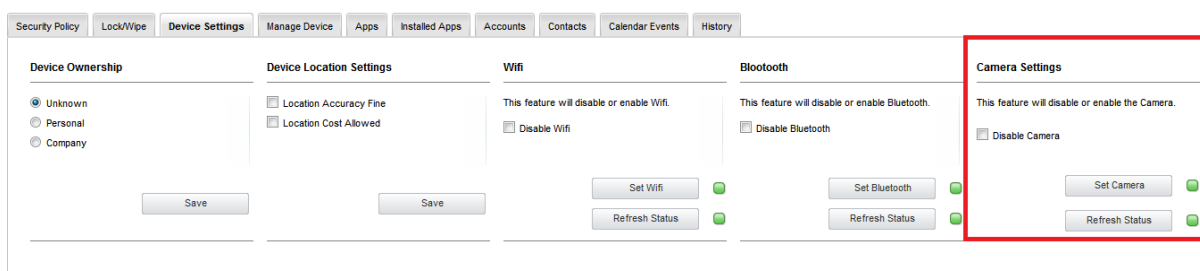
## 11.8. Manage Bluetooth

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



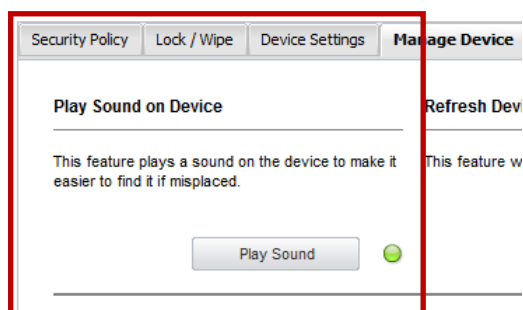
## 11.9. Manage Camera on Android

This feature can disable the camera of the Android device.



## 11.10. Play Sound on Device for Android

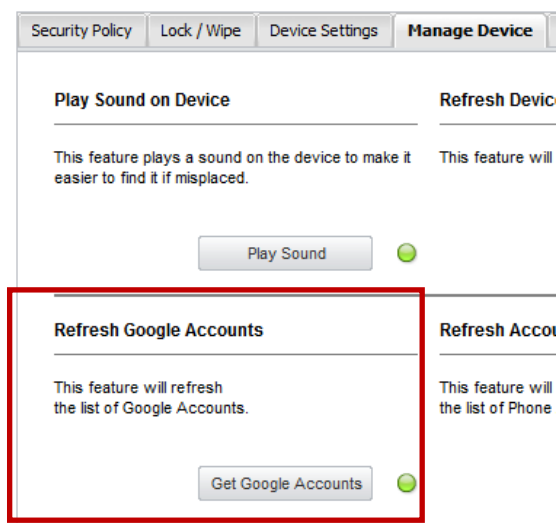
Mobile Devices > Manage Device > Play Sound on Device



The option "Play Sound" will make the Android device play a loud noise in order to locate a misplaced device.

## 11.11. Refresh Google Accounts for Android

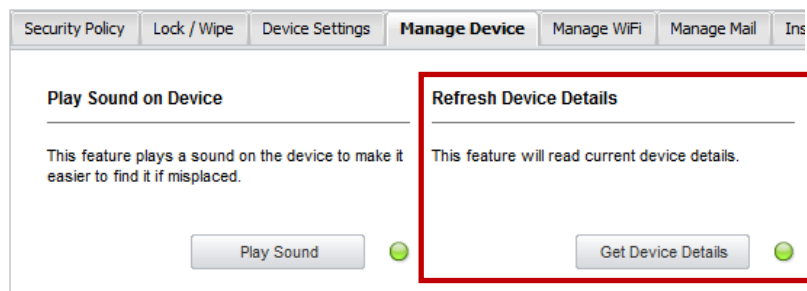
Mobile Devices > Manage Device > Refresh Google Accounts



The option Refresh Google Accounts by clicking “Get Google Accounts” will receive a list of Google accounts registered with the Android device. The list of Accounts is displayed under Mobile Devices > Manage Device > Accounts.

## 11.12. Refresh Device Details for Android

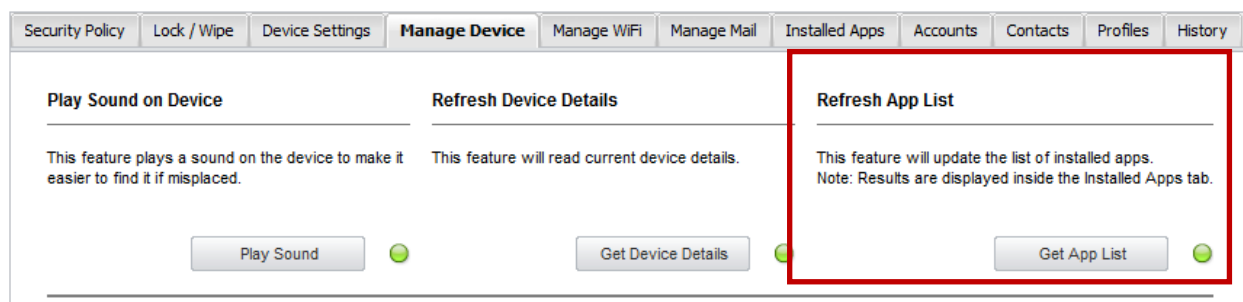
Mobile Devices > Manage Device > Refresh Device Details



This function will ask the Android devices for its latest details and display them in the Mobile Device Information section. This function is particularly useful if all device information is not displayed after enrollment.

## 11.13. Refresh App List for Android

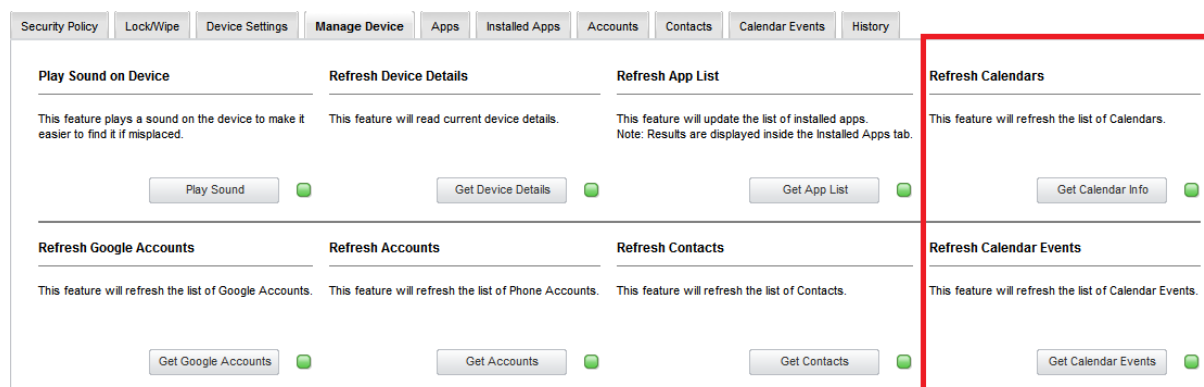
Mobile Devices > Manage Device > Refresh App List



This function by clicking “Get App List” 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 > Installed Apps

## 11.14. Manage Calendar Events

Through this feature it is possible to manage the Calendar Events on an Android device. The list of the existing events can be requested by pushing the “Get Calendar Info” and “Get Calendar Events” buttons.



The administrator will see the events in the “Calendar Events” section. In the screenshot below we did not push the “Get Calendar Info” button, so only the “Calendar Events” are listed (note that the “Calendar Name” field is empty). If we would push the button afterwards, the “Calendar Name” field would also get completed.

Security Policy Lock/Wipe Device Settings Manage Device Apps Installed Apps Accounts Contacts <b>Calendar Events</b> History												
Results												
Title ▾	Calendar Name	Event Start	Event End	Timezone	Whole Day	Location	Description	Alarm Set	Status	Visibility	Overlap	Act
The Three Holy Hierarchs	-	30 January 2014 1:00	31 January 2014 1:00	UTC	✓				Tentative	Default	No overlaps	✗
The Three Holy Hierarchs	-	30 January 2015 1:00	31 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	✗
The Restoration of Democracy	-	24 July 2013 2:00	25 July 2013 2:00	UTC	✓				Tentative	Default	No overlaps	✗
The Ochi day	-	28 October 2014 1:00	29 October 2014 1:00	UTC	✓				Tentative	Default	No overlaps	✗
Synaxis of the Mother of God	-	26 December 2014 1:00	27 December 2014 1:00	UTC	✓				Tentative	Default	No overlaps	✗
Polytechnieo	-	17 November 2013 1:00	18 November 2013 1:00	UTC	✓				Tentative	Default	No overlaps	✗
Polytechnieo	-	17 November 2014 1:00	18 November 2014 1:00	UTC	✓				Tentative	Default	No overlaps	✗
New Year's Day	-	1 January 2015 1:00	2 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	✗
Labor Day / May Day	-	1 May 2013 2:00	2 May 2013 2:00	UTC	✓				Tentative	Default	No overlaps	✗
Labor Day / May Day	-	1 May 2014 2:00	2 May 2014 2:00	UTC	✓				Tentative	Default	No overlaps	✗
Good Friday	-	18 April 2014 2:00	19 April 2014 2:00	UTC	✓				Tentative	Default	No overlaps	✗
First entry	-	8 January 2014 7:00	8 January 2014 8:00	Europe/Athens					Tentative	Default	No overlaps	✗
Epiphany	-	6 January 2015 1:00	7 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	✗
Easter Sunday	-	5 May 2013 2:00	6 May 2013 2:00	UTC	✓				Tentative	Default	No overlaps	✗
Easter Sunday	-	20 April 2014 2:00	21 April 2014 2:00	UTC	✓				Tentative	Default	No overlaps	✗
Dormition of the Holy Virgin	-	15 August 2013 2:00	16 August 2013 2:00	UTC	✓				Tentative	Default	No overlaps	✗

## 11.15. 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 11.13 Refresh App List for Android.

Security Policy Lock / Wipe Device Settings Manage Device Manage WiFi Manage Mail <b>Installed Apps</b> Accounts Contacts Profiles History						
Results						
Name ▾	Identifier	Version	Short Version	Last Status	Actions	
alogcat	org.tb.alogcat	2.6.1	2.6.1	Apps List Update	✗	✓
EPP Client	com.cososys.eppclient	1.0.0.4	1.0.0.4	Apps List Update	✗	✓
Google Play services	com.google.android.gms	1.0.13	1.0.13	Apps List Update	✗	✓
3 results [ 50 ▾ per page]						

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

### 11.15.1. Removing Installed Apps on Android

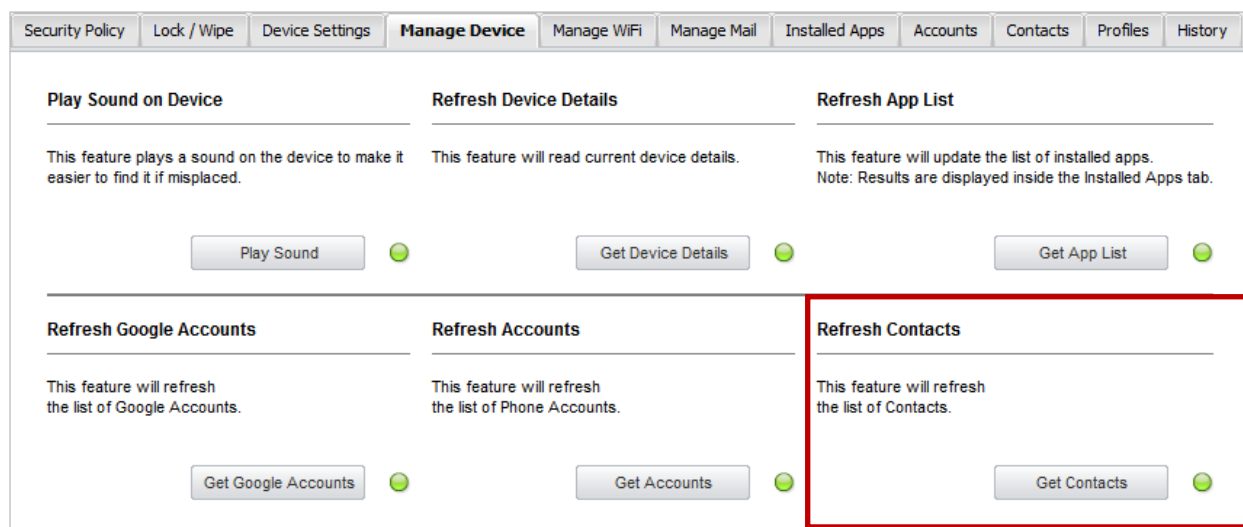
The Endpoint Protector Administrator can send an action to the Android device and ask the device to remove the app from the device. By clicking the ✗ „Remove App" button the request is sent to the device. The Android device will now show the user that the device is supposed to be removed. The user can 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.

## 11.16. 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 “Get Contacts” under the option Mobile Devices > Manage Devices > Refresh Contacts.



## 11.17. Get Accounts on Android

Mobile Devices > Accounts

The tab “Accounts” Lists all accounts used on an Android device.

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

## 11.18. History of Android Device Actions

Mobile Devices > History

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

Htc_europe HTC Wildfire S A510e	SetMaximumTimeToLock		Success	24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetMaximumFailedPasswordsForWipe		Success	24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetPasswordMinimumLength		Success	24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetPasswordQuality		Success	24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	AskUserChangePassword		Success	24 October 2012 15:05
Htc_europe HTC Wildfire S A510e	GetContacts		Success	24 October 2012 15:05
Htc_europe HTC Wildfire S A510e	GetAccounts		Success	24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetGoogleAccounts		Success	24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetInstalledPackages		Success	24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetDeviceInfo		Success	24 October 2012 15:04

## 11.19. Manage WiFi, Manage Mail, Profiles on Android

Mobile Devices > Manage WiFi

Mobile Devices > Manage Mail

Mobile Devices > Profiles

The tabs “Manage WiFi”, “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 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with various options, including 'iOS App Management' which is highlighted with a red box. The main content area is titled 'Mobile Device Management - iOS App Management' and features a search bar for the iTunes App Store. Below the search bar, there is a table of search results for 'EPP MDM' by CoSoSys, version 1.0.0.6. At the bottom, there is a section for 'Manage iOS Apps' showing a table with the same app details.

**Endpoint Protector** | 4 Reporting and Administration Tool

**Mobile Device Management - iOS App Management**

**Search iTunes App Store**

Search:  Search type: Using search term County: United States

**Search Results**

Select	Icon	Title	Vendor	Version	Description
<input type="checkbox"/>		EPP MDM	CoSoSys	1.0.0.6	Endpoint Protector Mobile Device Ma

**Manage iOS Apps**

OS	Icon	Title	Vendor	Version	Description
iOS		EPP MDM	CoSoSys	1.0.0.6	Endpoint Protector Mobile Device Management provides com

1 result [ 10 per page]



## 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 select “Using search term” or “Using iTunes App ID”.

The screenshot displays the Endpoint Protector 4 Reporting and Administration Tool interface. The left sidebar contains various navigation options, including Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Enroll Devices, Mobile Devices, MDM Policies, iOS App Management, APNS Certificate Setup (Apple), GCM/Maps Setup (Google), Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Mobile Device Management - iOS App Management'. A red box highlights the 'Search iTunes App Store' section, which includes a search bar, a dropdown for 'Search type' (set to 'Using search term'), a dropdown for 'Country' (set to 'United States'), and a 'Search App Store' button. Below this, the 'Search Results' table shows one result: 'EPP MDM' by 'CeSoSys' with version '1.0.0.6'. At the bottom, the 'Manage iOS Apps' table also lists 'EPP MDM'.

Select	Icon	Title	Vendor	Version	Description
<input type="checkbox"/>		EPP MDM	CeSoSys	1.0.0.6	Endpoint Protector Mobile Device Management provides complete iOS enterprise mob ...

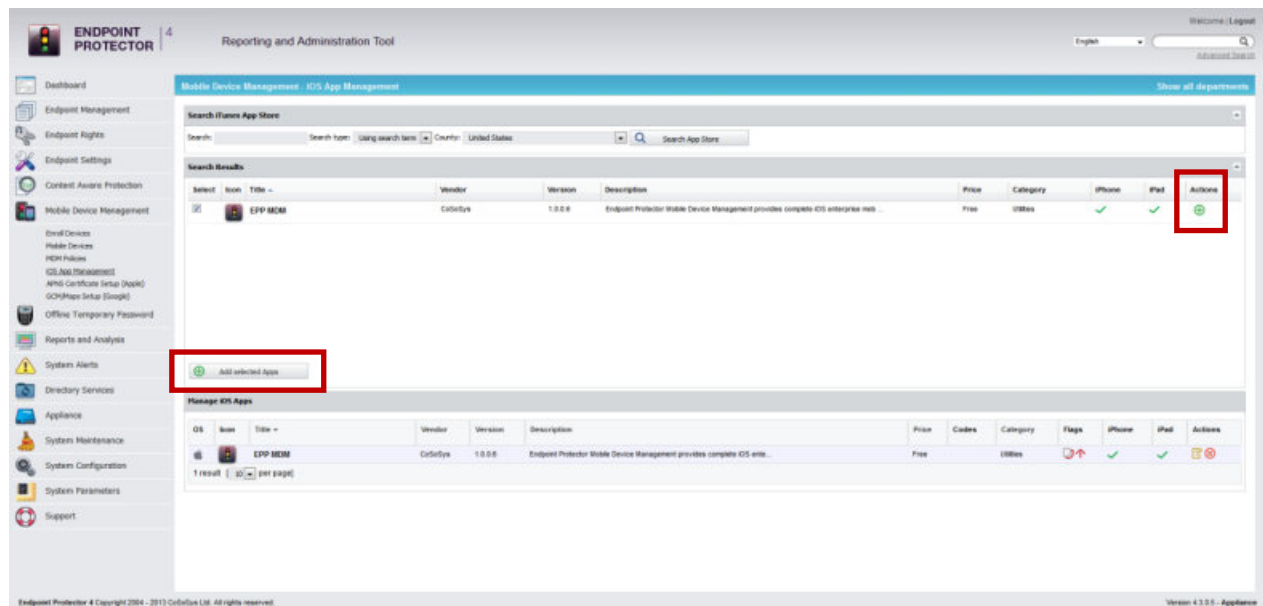
  

OS	Icon	Title	Vendor	Version	Description
iOS		EPP MDM	CeSoSys	1.0.0.6	Endpoint Protector Mobile Device Management provides complete iOS ente ...

1 result | 10 per page

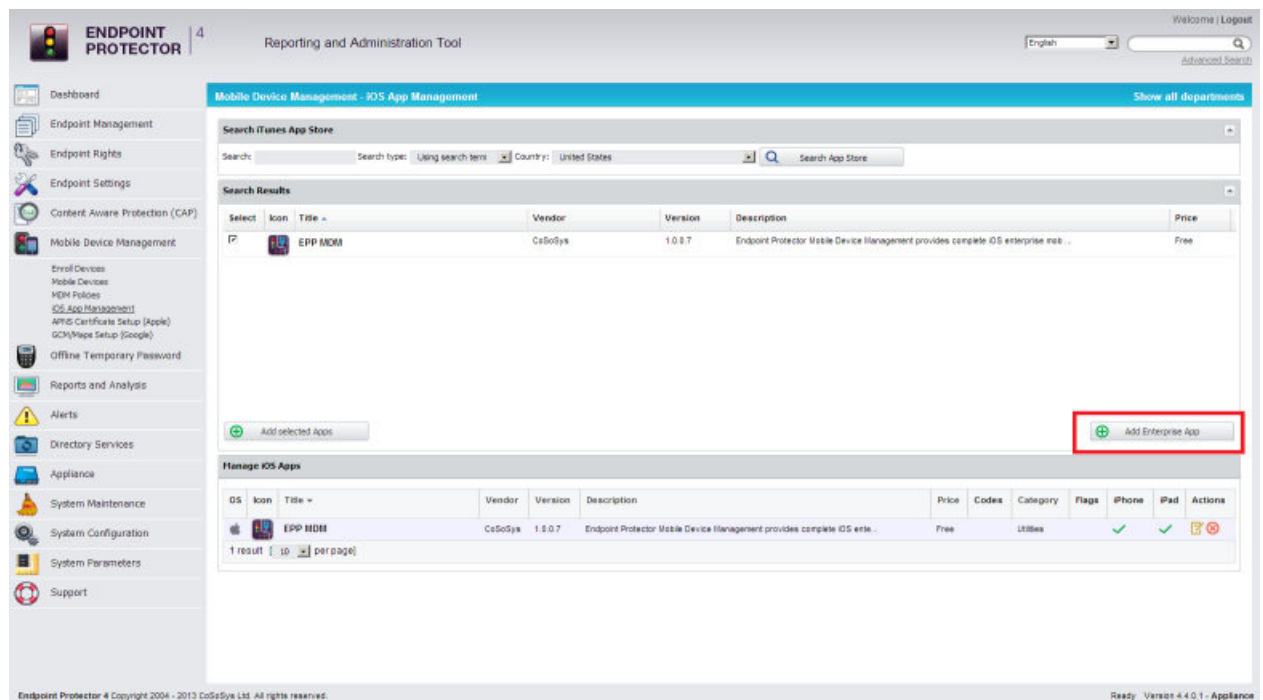
### 12.1.2. Adding Apps to Managed Apps Catalog

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

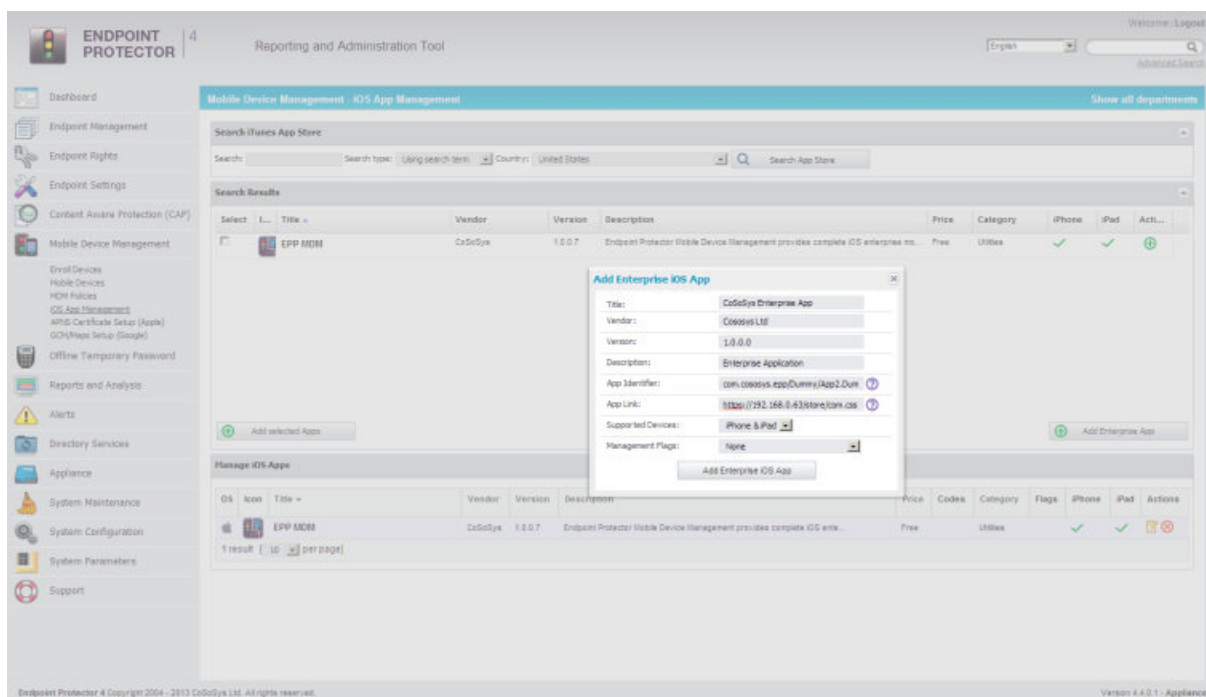


### 12.1.3. Adding „Enterprise Apps“ to Managed Apps Catalog

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

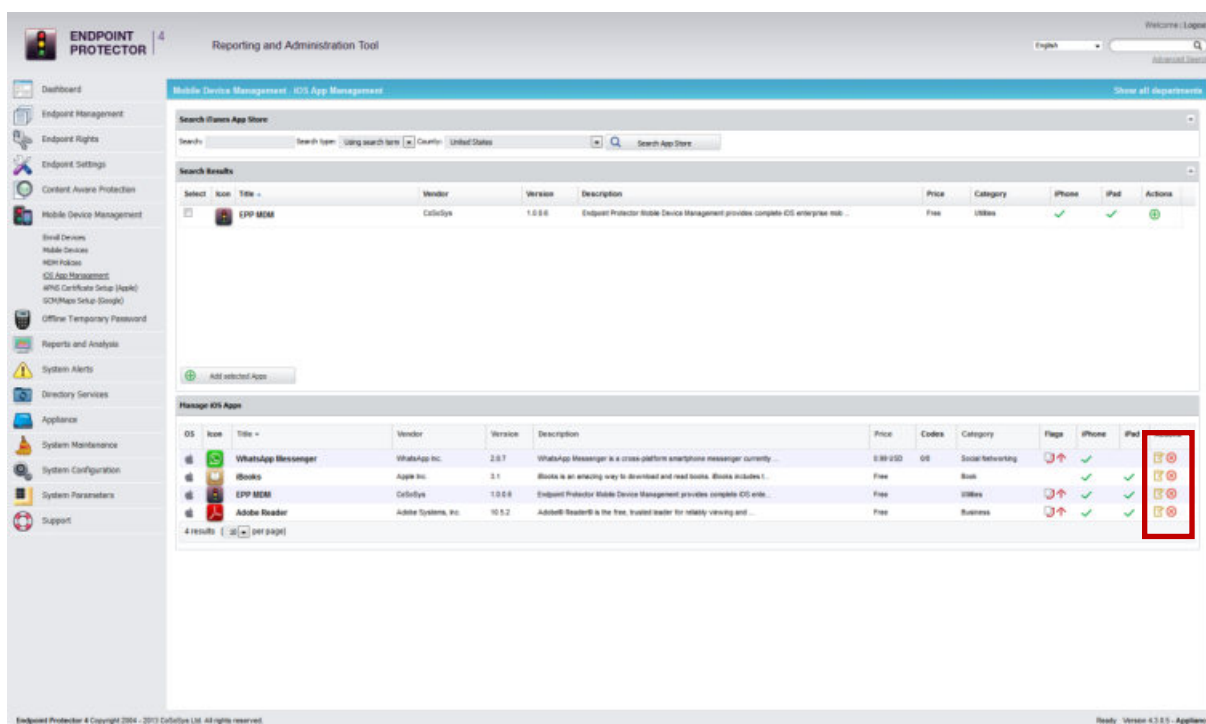




You will have to enter the required details in the pop-up window.



## 12.2. Editing App Management Options

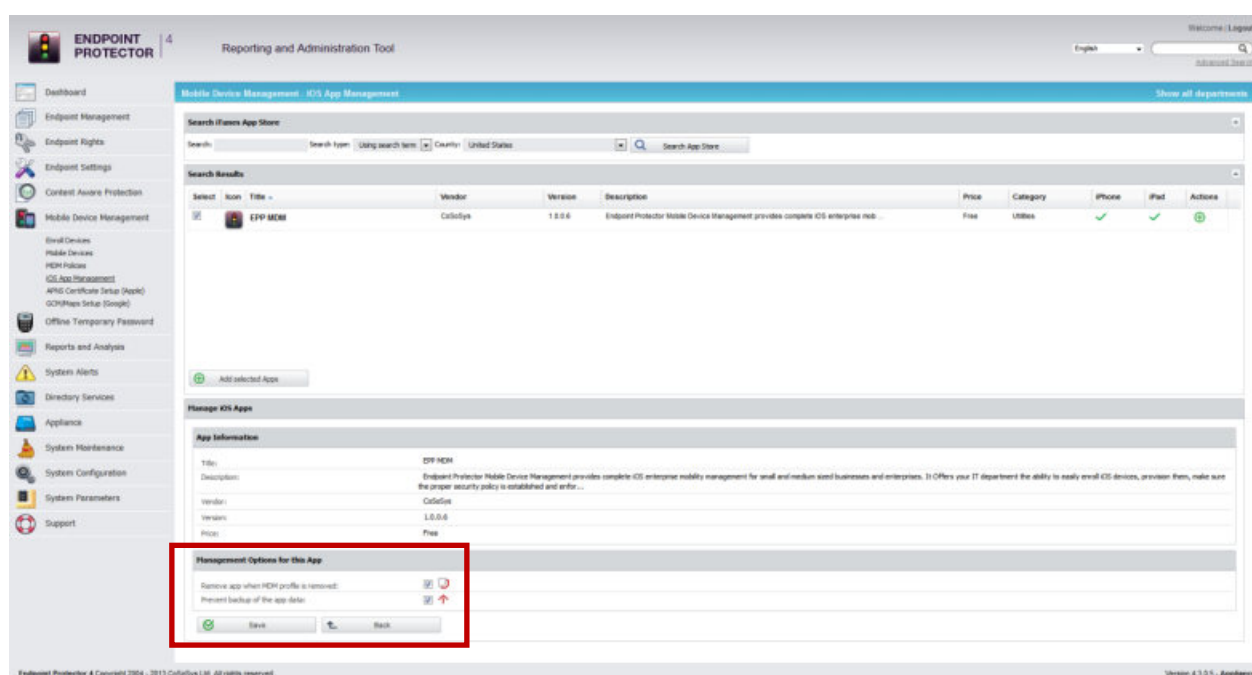
Managed Apps options can be modified by selecting "Edit App".



Management Options for this App	
Remove app when MDM profile is removed:	<input checked="" type="checkbox"/> 
Prevent backup of the app data:	<input checked="" type="checkbox"/> 

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.



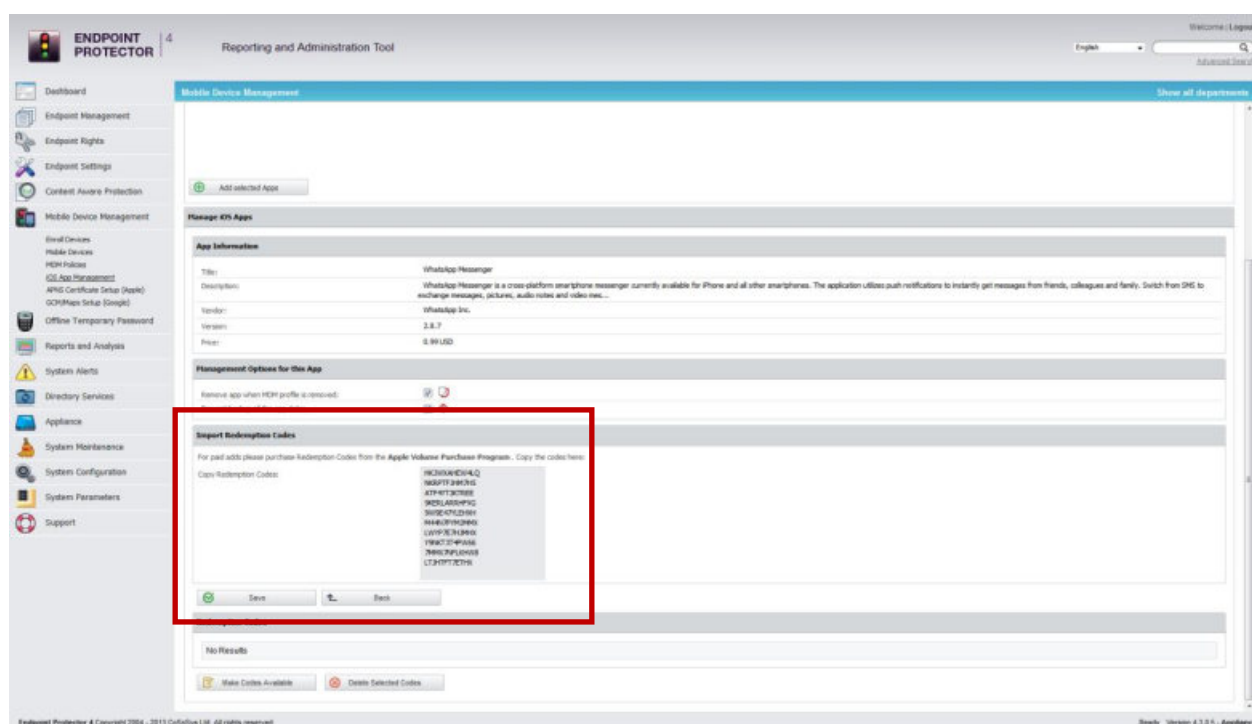
The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The left sidebar contains navigation links for Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Email Devices, Mobile Devices, MDM Policies, iOS App Management, Apple Certificate Setup (Apple), Google Apps Setup (Google), Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Mobile Device Management - iOS App Management'. It features a search bar for the iTunes App Store, a table of search results for 'EPP MDM' (version 1.0.0.6), and a section for managing this app. The 'Management Options for this App' section is highlighted with a red box, showing the same options as the top of the page: 'Remove app when MDM profile is removed' and 'Prevent backup of the app data', both with checked checkboxes and corresponding icons. The bottom of the interface shows the footer with 'Endpoint Protector 4 Copyright 2004 - 2013 Collopy LLC All rights reserved.' and 'Version 4.3.0.5 - Appliance'.

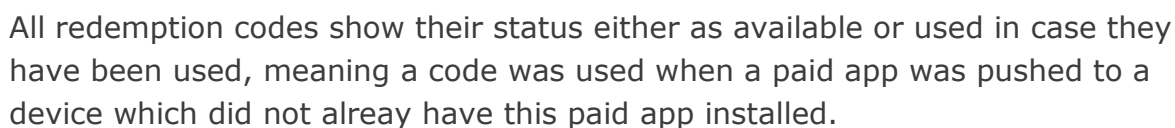
## 12.3. Managed Paid Apps

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.



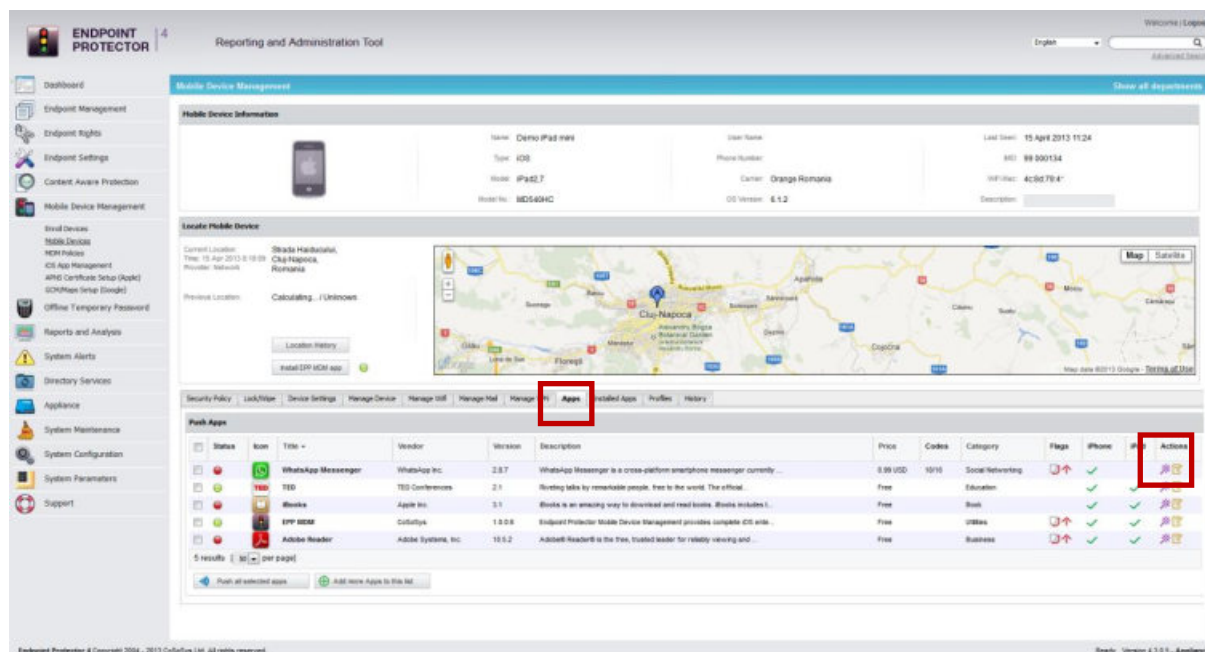


Additionally the number of total and still available (not yet consumed) redemption codes is shown in the column "Codes" in the list of "Managed iOS Apps". In the example below 10/10 meaning ten of ten codes are available.


Manage iOS Apps												
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 ...	\$99 USD	1010	Social Networking				 
		iBooks	Apple Inc.	3.1	iBooks is an amazing way to download and read books. iBooks includes L...	Free		Book				 
		EPP MDM	CaSeSys	1.0.8.6	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				 
4 results <span>[ 12 ]</span> per page												

## 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”.



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.

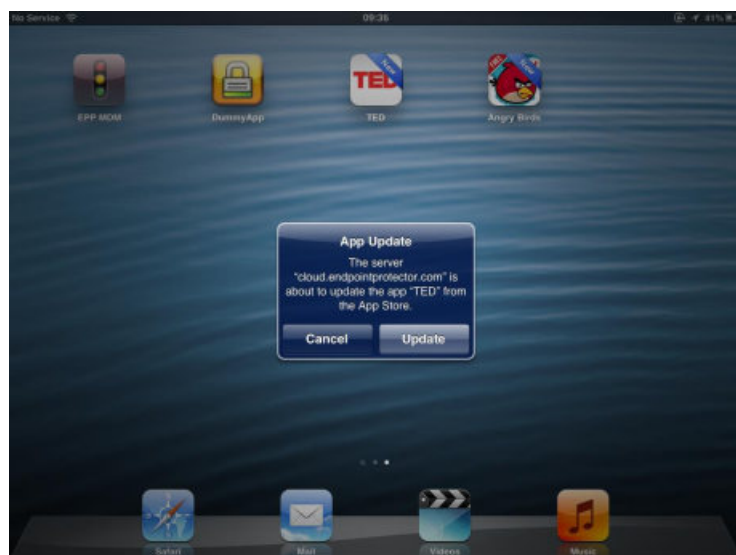


Apps can also be pushed from MDM policies “Manage Apps” tab.



### 12.4.1. Update Managed Apps / Changing Settings

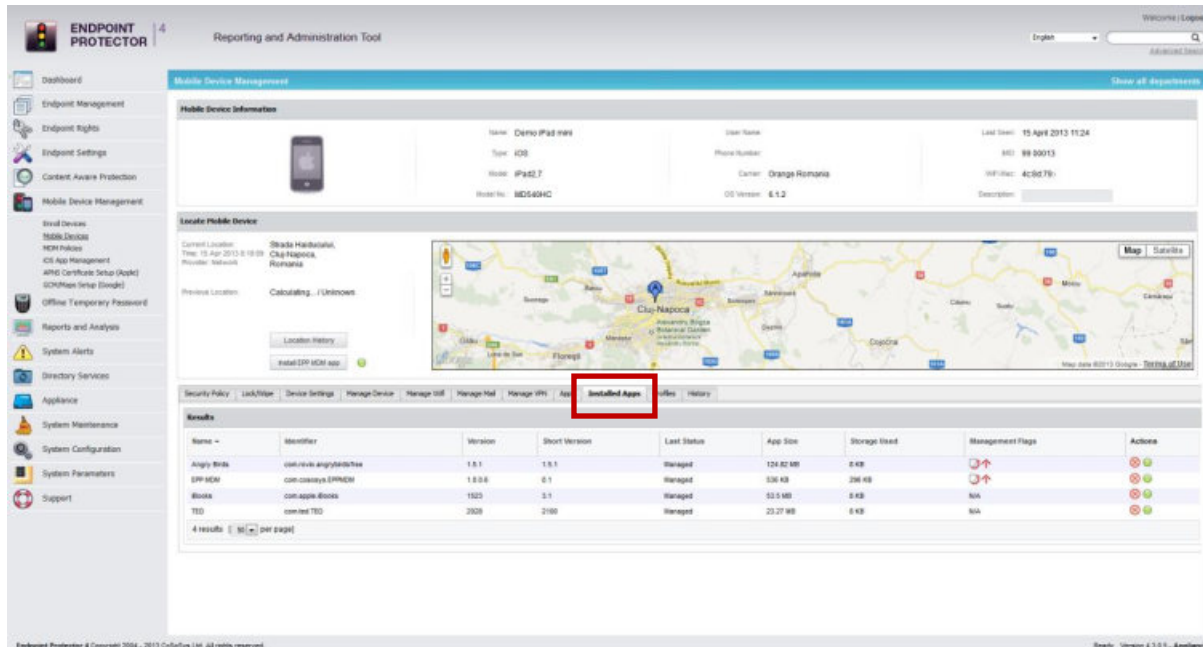
In case a newer version of an app is available you can update it using the same steps as when pushing a new app to a managed device. In case an update is pushed the user will be prompted to update the app. In case of paid apps no new redemption code is consumed during this process.





## 12.5. Removing Managed Apps from iOS Devices

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



The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The left sidebar contains navigation options: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Email Devices, Mobile Policies, iOS App Management, MDM Certificate Setup (Apple), MDM Certificate Setup (Google), Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, AppStore, System Maintenance, System Configuration, System Parameters, and Support.


The main content area is titled "Mobile Device Management" and shows details for a device named "Demo iPad Mini". The device information includes: Name: Demo iPad Mini, Type: iOS, Model: iPad2,7, Model No: MD540MC, User Name, Phone Number, Last Seen: 15 Apr 2013 11:24, IMEI: 89 80013, SIM: 4c5679, Carrier: Orange Romania, and OS Version: 6.1.2.

Below the device information is a map showing the current location of the device, labeled "Cluj Napoca, Romania". The map also shows the previous location, "Cibadling, Unknown".

The "Installed Apps" tab is selected, showing a table of installed applications. The table has columns: Name, Identifier, Version, Short Version, Last Status, App Size, Storage Used, Management Flags, and Actions. The table lists four apps: Angry Birds, EPP MDM, iBooks, and TED.

Name	Identifier	Version	Short Version	Last Status	App Size	Storage Used	Management Flags	Actions
Angry Birds	com.riviera.angrybirdsfree	1.0.1	1.0.1	Managed	124.82 KB	0 KB	⬆️⬆️	ⓧ️ⓧ️
EPP MDM	com.casatop.EPPMDM	1.0.0.0	0.1	Managed	536 KB	296 KB	⬆️⬆️	ⓧ️ⓧ️
iBooks	com.apple.iBooks	1023	3.1	Managed	53.5 MB	0 KB	N/A	ⓧ️ⓧ️
TED	com.net.TED	2008	2.100	Managed	23.27 KB	0 KB	N/A	ⓧ️ⓧ️

At the bottom of the table, it says "4 results (1/1 over page)".

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 Android apps. Mobile Apps can be managed under the following option  
Mobile Device Management > Android App Management.

The screenshot displays the Endpoint Protector 4.4.0.3 web interface. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Welcome | Logout' and 'Advanced Search' links. The left sidebar contains a menu with categories: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The 'Mobile Device Management' section is expanded, showing sub-options like Dashboard, Enroll Devices, Mobile Devices, MDM Policies, iOS App Management, **Android App Management** (highlighted), APNS Certificate Setup (Apple), GCM/Maps Setup (Google), and Offline Temporary Password. The main content area is titled 'Mobile Device Management - Android App Management' and includes a 'Show all departments' link. It features a table titled 'Android Apps' with columns for OS, Title, Vendor, Version, Description, and Actions. A single entry is shown: 'CeSoSys Notepad Demo' by 'CeSoSys' with version '1.0'. Below the table is a pagination bar showing '1 result' and '50 per page'. An 'Add Android App' button is located below the table. The footer contains the copyright notice 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and the status 'Ready Version 4.4.0.3 - Appliance'.

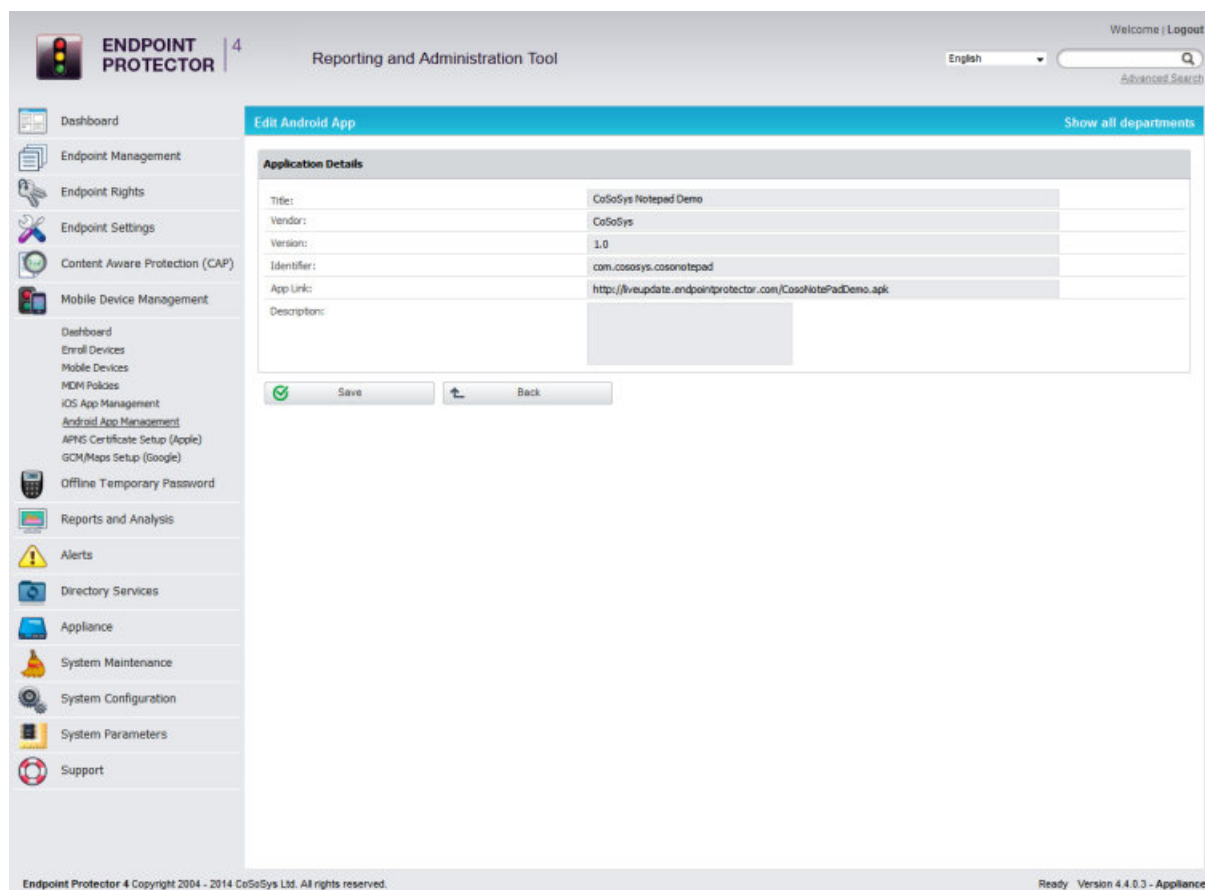
OS	Title	Vendor	Version	Description	Actions
	CeSoSys Notepad Demo	CeSoSys	1.0		

1 result [ 50 per page]

[Add Android App](#)

## 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.







The screenshot shows the 'Edit Android App' form in the Endpoint Protector 4 Reporting and Administration Tool. The form is titled 'Edit Android App' and has a 'Show all departments' link. The form contains the following fields:

- Title: CoSoSys Notepad Demo
- Vendor: CoSoSys
- Version: 1.0
- Identifier: com.cososys.cosonotepad
- App Link: http://liveupdate.endpointprotector.com/CosonotepadDemo.apk
- Description: (empty)

At the bottom of the form, there are 'Save' and 'Back' buttons. The 'App Link' field is highlighted with a red box.

## 13.2. Editing App Management Options

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


Mobile Device Management - Android App Management					Show all departments
Android Apps					
OS	Title ▾	Vendor	Version	Description	Actions
	CoSoSys Notepad Demo	CoSoSys	1.0		 
1 result [ 50 ▾ per page]					
 Add Android App					

## 13.3. 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.

The screenshot shows the Endpoint Protector 4 web interface. The top navigation bar includes the logo, version number 4, and the title 'Reporting and Administration Tool'. The left sidebar contains a menu with options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), and Mobile Device Management. The main content area is titled 'Mobile Device Management - Android App Management'. It features a 'Mobile Device Information' section with details for a Samsung GT-I9505, including user 'tony', phone number '123456', carrier 'RO ORANGE', and OS version '4.3'. Below this is a 'Locate Mobile Device' section showing the current location as 'Strada Haiducului, Cluj-Napoca 400000, Romania' and a map. At the bottom, there is a table of 'Android Apps' with one entry: 'CoSoSys Notepad Demo' by 'CoSoSys' version '1.0'. The 'Actions' column for this app shows a push icon. Below the table are buttons for 'Push all selected apps' and 'Add more Apps to this list'.

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.

## 13.4. 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 4 web interface. The left sidebar contains navigation links: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Dashboard, Enroll Devices, Mobile Devices, MDM Policies, iOS App Management, Android App Management, APNS Certificate Setup (Apple), GCM/Maps Setup (Google), Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support.

The main content area is titled "Mobile Device Management" and includes a "Show all departments" link. It features a "Mobile Device Information" section for a Samsung GT-I9505, showing details like User Name (Tony), Phone Number (123456), Carrier (RO ORANGE), and OS Version (4.3). Below this is a "Locate Mobile Device" section with a map showing the current location in Cluj-Napoca, Romania.

The "Installed Apps" tab is selected, displaying a table of installed applications. The table has columns for Name, Identifier, Version, Short Version, Last Status, App Size, Storage Used, Management Flags, and Actions. The Actions column contains a red 'X' icon for removal and a green checkmark for status.

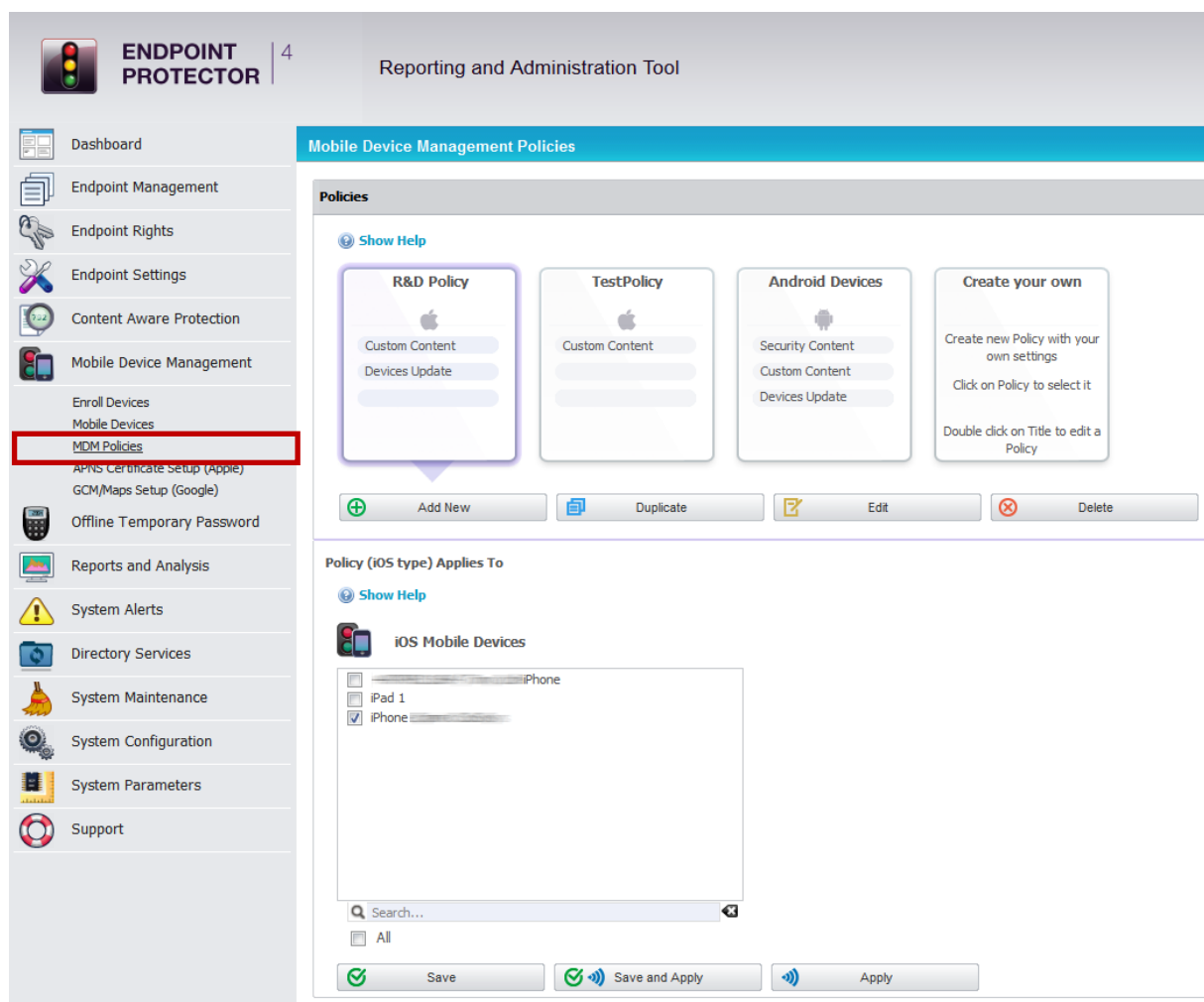
Name	Identifier	Version	Short Version	Last Status	App Size	Storage Used	Management Flags	Actions
100 Doors 2013	com.ginnetx.stages	1.4.3	1.4.3	App List Update	N/A	N/A	N/A	[X] [✓]
Alens Space	com.ginnetx.alensspace	1.0.0	1.0.0	App List Update	N/A	N/A	N/A	[X] [✓]
EPP Client	com.cossays.eppclient	1.0.0.0	1.0.0.0	App List Update	N/A	N/A	N/A	[X] [✓]
Galaxy S4 Sensors	pl.konur.android.galaxy4sensors	1.0	1.0	App List Update	N/A	N/A	N/A	[X] [✓]
Hot Mod	com.gamenet.hotmod	1.5	1.5	App List Update	N/A	N/A	N/A	[X] [✓]
NotePad	com.example.android.nolepad	null	null	App List Update	N/A	N/A	N/A	[X] [✓]
Pinterest	com.pinterest	2.4.4	2.4.4	App List Update	N/A	N/A	N/A	[X] [✓]
Pulse	com.alphonso.pulse	4.0.0	4.0.0	App List Update	N/A	N/A	N/A	[X] [✓]

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.3 - Appliance

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 manage 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.

**Add a new Policy** Show all departments

Policy Device Type: ☒ iOS ☐ Android

**Policy Information**

Policy Name:

Policy Description:

iOS Version: ☐ iOS6 and older ☒ iOS7 and newer

Supervised Devices: ☐ No ☒ Yes

**Security Policy** **Device Settings** **Manage Device** **Manage WiFi** **Manage Apps**

**Set Security Policy**

☐ Clear Password (No more password required)

Simple Value: ☐ This feature will reset the current device password to be empty, hence the device can be unlocked without entering a password.

Alphanumeric Password: ☐

Min Password Length:

Min Number Of Complex Chars:

Max Password Age (days):

Max Time To Lock (minutes):

Password History:

Grace Period (minutes):

Max Failed Password Retries:

Enable/Disable: ☐

**Set Restriction Policy**

**All:**

☐ **Device Functionality**

Allow installing apps: ☐

Allow Siri: ☐

Allow Siri while device locked: ☐

Allow use of camera: ☐

Allow FaceTime: ☐

Allow screen capture: ☐

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: ☐

☐ **Applications**

Allow YouTube: ☐

Allow iTunes: ☐

Allow Safari: ☐

Allow Safari Auto Fill: ☐

Allow javascript on Safari: ☐

Allow popups on Safari: ☐

Safari fraud warning: ☐

☐ **iCloud**

Allow iCloud backup: ☐

Allow iCloud document sync: ☐

Allow photo stream: ☐

Allow shared photo streams: ☐

☐ **Security and Privacy**

Allow sending diagnostic data: ☐

Allow untrusted TLS certificate: ☐

Force encrypted backups: ☐

☐ **Content Rating**

Allow explicit content: ☐

☐ **iOS7 Restrictions**

Allow fingerprint for unlock: ☐

Allow Control Center on Lock Screen: ☐

Allow Lock Screen Notifications: ☐

Allow Lock Screen Today View: ☐

Allow managed docs in unmanaged Apps: ☐

Allow unmanaged docs in managed Apps: ☐

Allow OTA PKG updates: ☐

Limit ad tracking: ☐

☐ **Supervised Devices 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: ☐

☒ Save

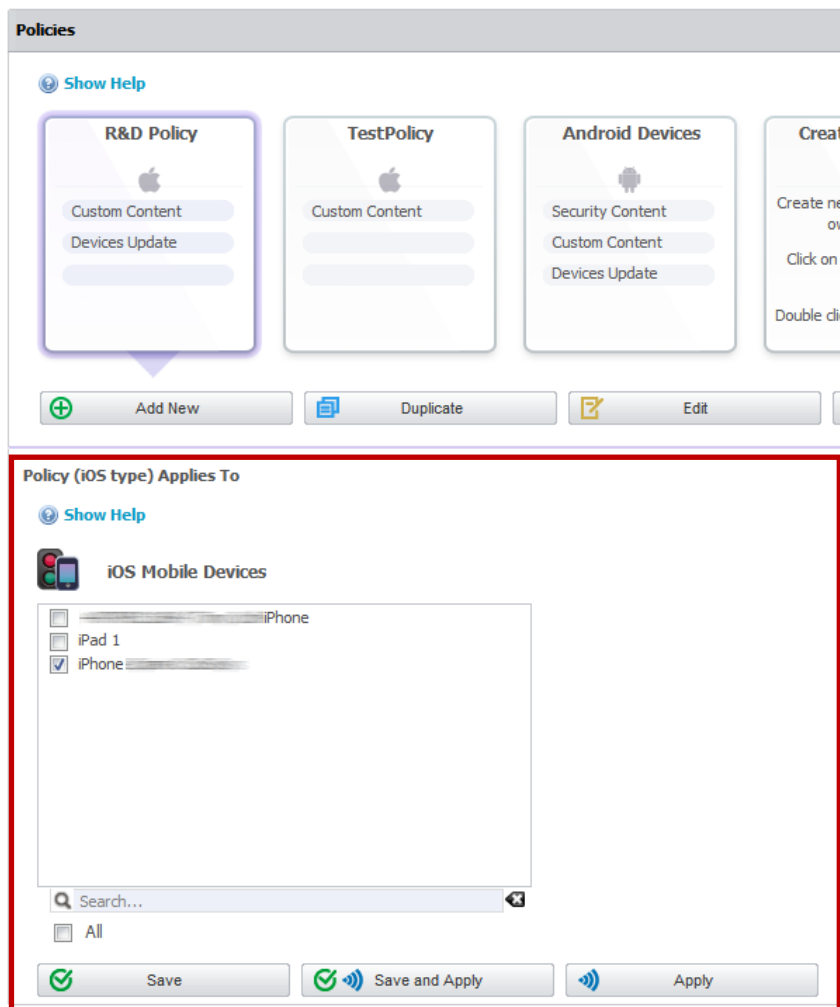
After you made the settings to the Policy click “Save”.

### 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.

#### **Attention!**

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.

#### **Attention!**

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

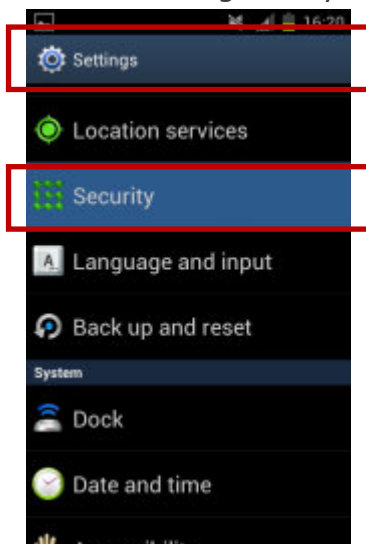
To uninstall the EPP MDM iOS app the user of the iOS device can uninstall it by pushing the EPP MDM app icon for two seconds and then deleting the app by clicking (x).

## 15.3. Android EPP Client App Uninstall / Unmanage Android Device

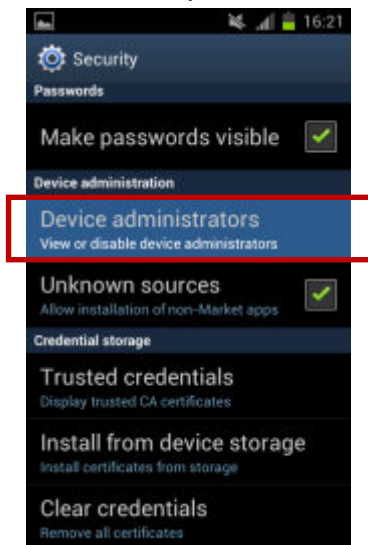
To uninstall EPP Client App on an Android Mobile Device, the user needs to disable the Device Administrator role from Device Settings.

To uninstall the EPP Client App follow these steps:

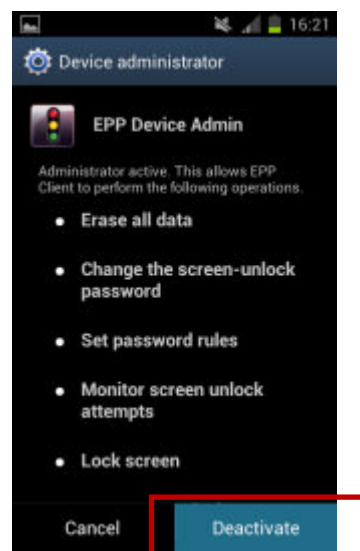
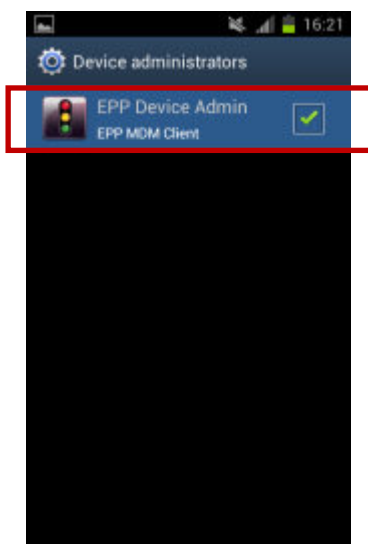
1. Go to "Settings" on your Android device and select "Security".



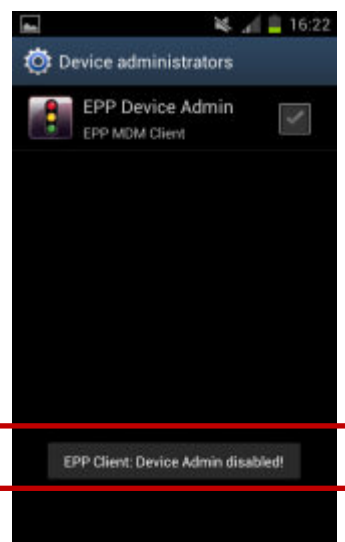
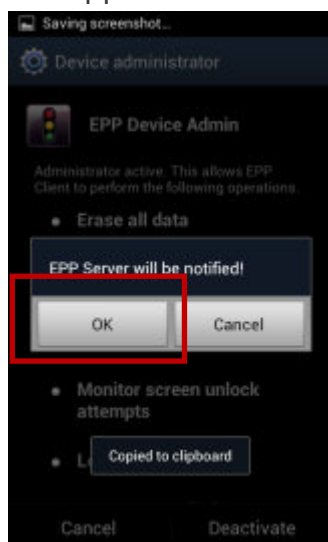
2. In "Security" select "Device administrators" and click on it.



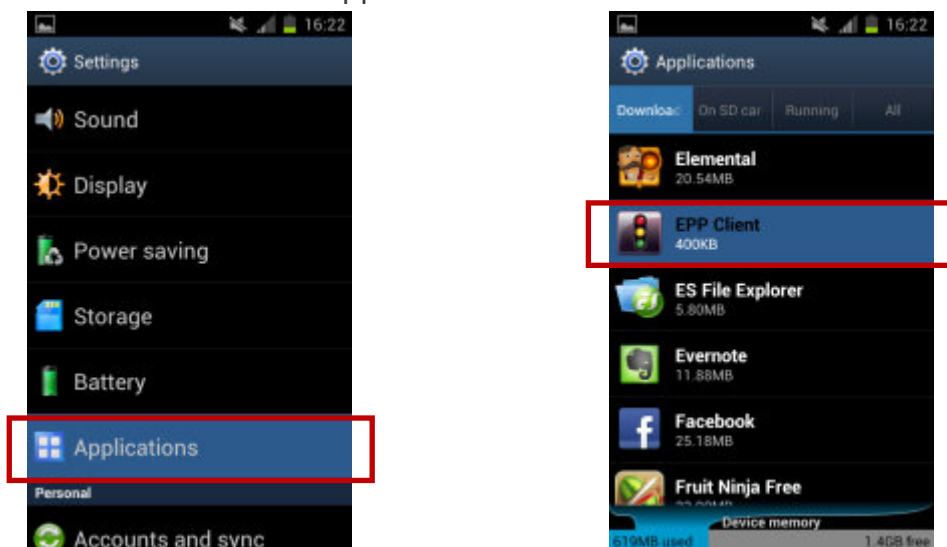
3. Select "EPP Device Admin" and click "Deactivate".



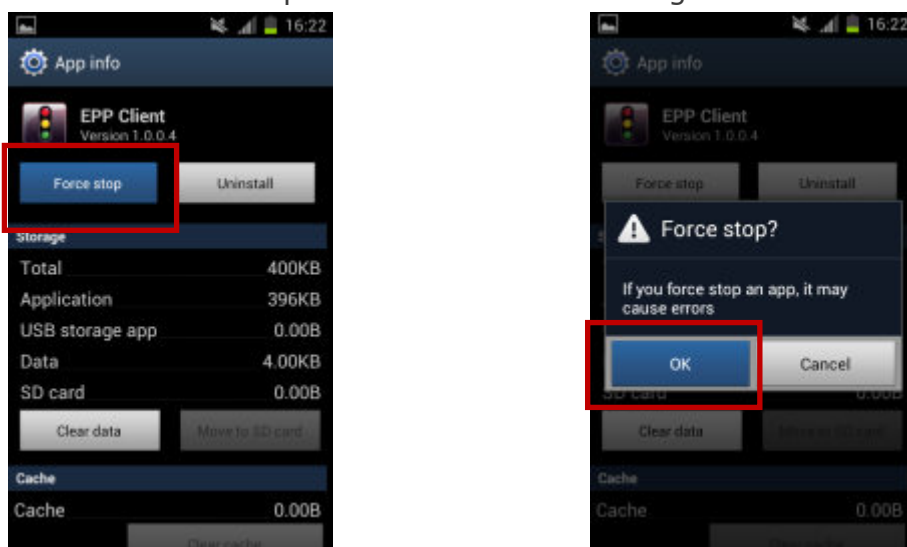
4. A pop-up will appear saying that the "EPP Server will be notified". To continue click "OK". A message saying "EPP Client Device Admin disabled" will appear.



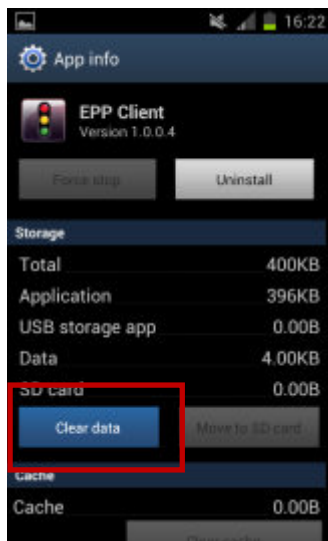
5. Now go to the “Application” menu on your Android device and locate “EPP Client” in the list of Applications. Click on “EPP Client”.



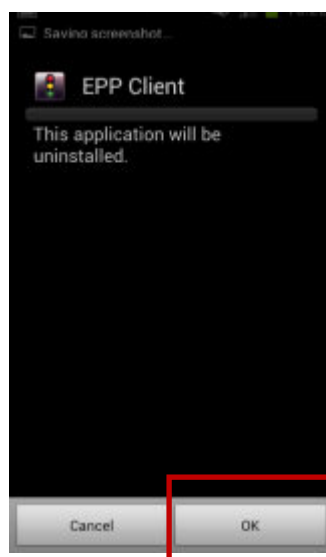
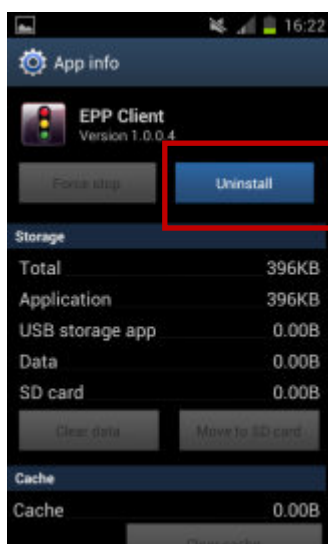
6. Click on “Force stop” and confirm the warning with “OK”.



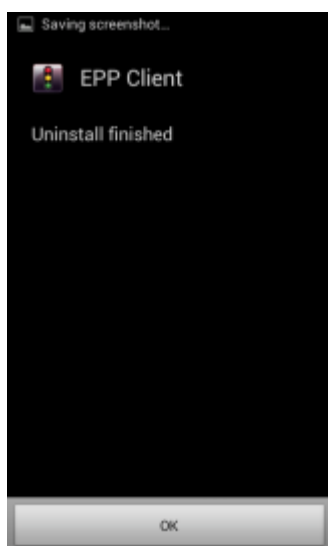
7. Now select “Clear data”.



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



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



### **Attention!**

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. GeoFencing

The Geofencing feature provides the option to define a virtual perimeter over a geographic area using a location-based service. This provides a better management of MDM Policies that apply only in a specific area.

The screenshot displays the Endpoint Protector 4 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Mobile Device Management - Geofencing' and includes a 'Manage Geofences' map view and an 'Available Map Features' table.

**Manage Geofences**

The map shows a geographical area with a black polygon representing a geofence. The map includes labels for various cities and regions, such as Denmark, Copenhagen, and Malmö.

**Available Map Features**

Type	Name	Description	Latitude	Longitude	Actions
Geofence	Geof2		56.12715420543736	19.4732666015625	[Icons]
Geofence	Geof1		55.49296107682209	17.4286095783125	[Icons]


2 results (50 per page)

Endpoint Protector 4 Copyright 2004 - 2014 CoSISys Ltd. All rights reserved. Ready Version 4.4.0.5


## 16.1. How to setup a GeoFence

Setting up the virtual perimeter is simple and intuitive.

To navigate on the map follow these steps:

1. Select the hand icon 
2. Click and drag the map to the desired location
3. Zoom in and out using the mouse scroll

To add a GeoFence follow these steps:

1. Select the shape icon 
2. Click to place the nodes that define the perimeter

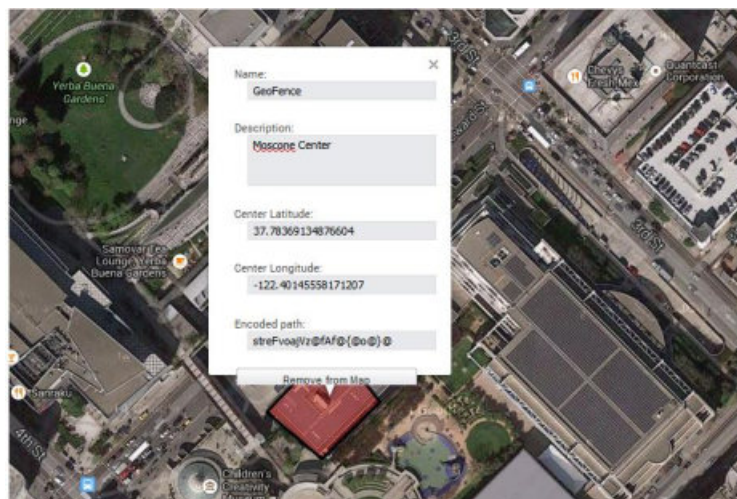
To save and edit a GeoFence follow these steps:

1. Click inside the above defined perimeter to edit and save details
2. Click on a node to delete or remove it from the map
3. Click on the Remove from Map button to remove GeoFence from the map
4. Click the Save Geofence Data to save the virtual perimeter

Remove from Map

Save Geofence Data

When a Geofence has been created, there are several details that are displayed to provide a better insight like Latitude and Longitude. There is also an optional Description field, recommended for a better management of the settings.





## 16.2. How to deploy MDM Policies using Geofences

Once the virtual perimeter has been defined, pushing specific settings through Geofences can be done from the MDM Policies.

### Mobile Device Management

#### Policy Device Type

Policy Device Type



#### Policy Information

Policy Name

test

Policy Description

iOS Version:

☒ iOS6 and older

☐ iOS7 and newer

Supervised Devices:

☒ No

☐ Yes

Security Policy

Device Settings

Manage Device

Manage WiFi

Manage Apps

Manage GeoFencing

Enable: ☒

#### Available GeoFences

<input type="checkbox"/>	Type	Name ▼	Description
<input checked="" type="checkbox"/>	Geofence	GeoFence	test
<input type="checkbox"/>	Geofence	GeoFence	

2 results [ 50 ▼ per page]



Save



Back



Delete

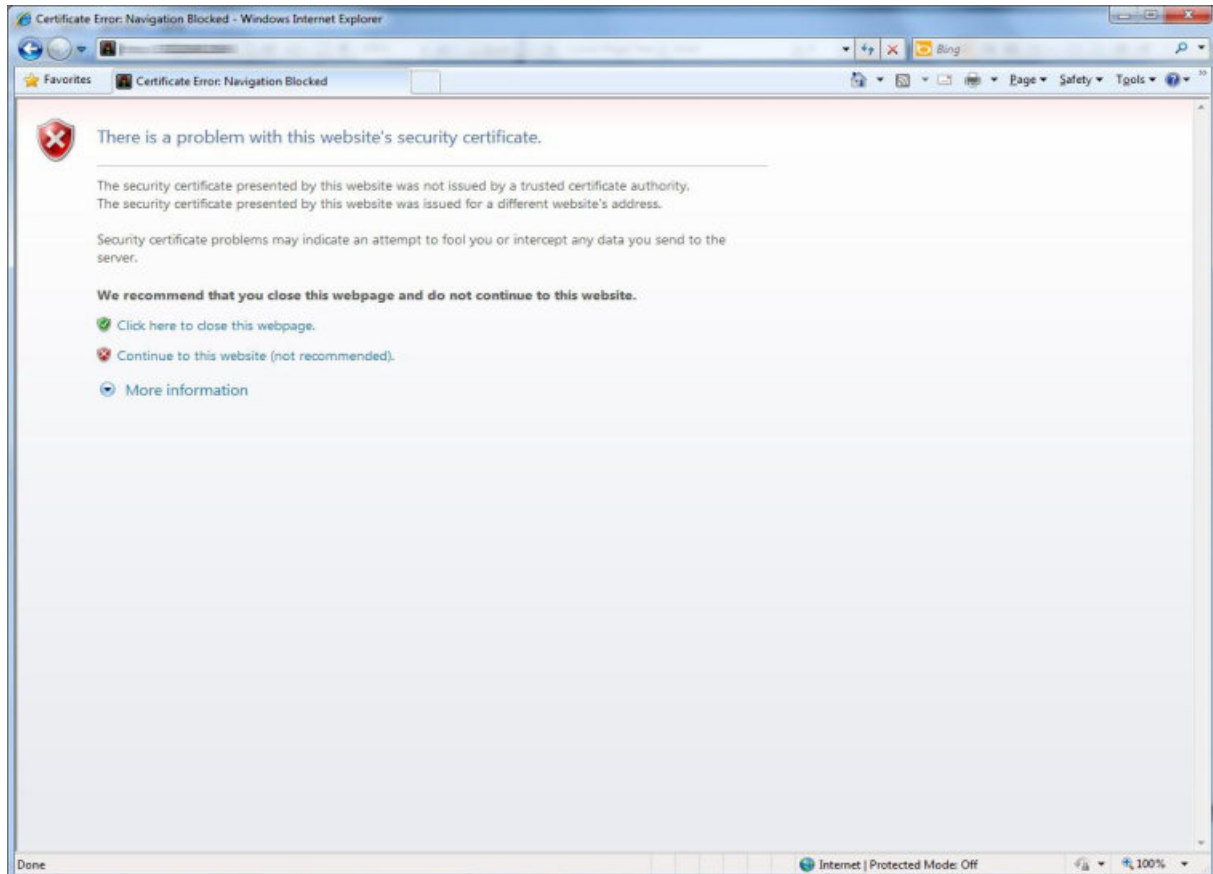
All off the settings previously defined in the Security Policy, Device Settings, Manage Device, Manage WiFi and Manage Apps tabs will apply to that specific Geofence.


# 17. Installing Root Certificate to your Internet Browser

## 17.1. For Microsoft Internet Explorer

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example <https://192.168.0.201>).

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.



Continue your navigation by clicking  "Continue to this website (not recommended)".

Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

Click the Certificate Error button just next to the IE address bar as shown.

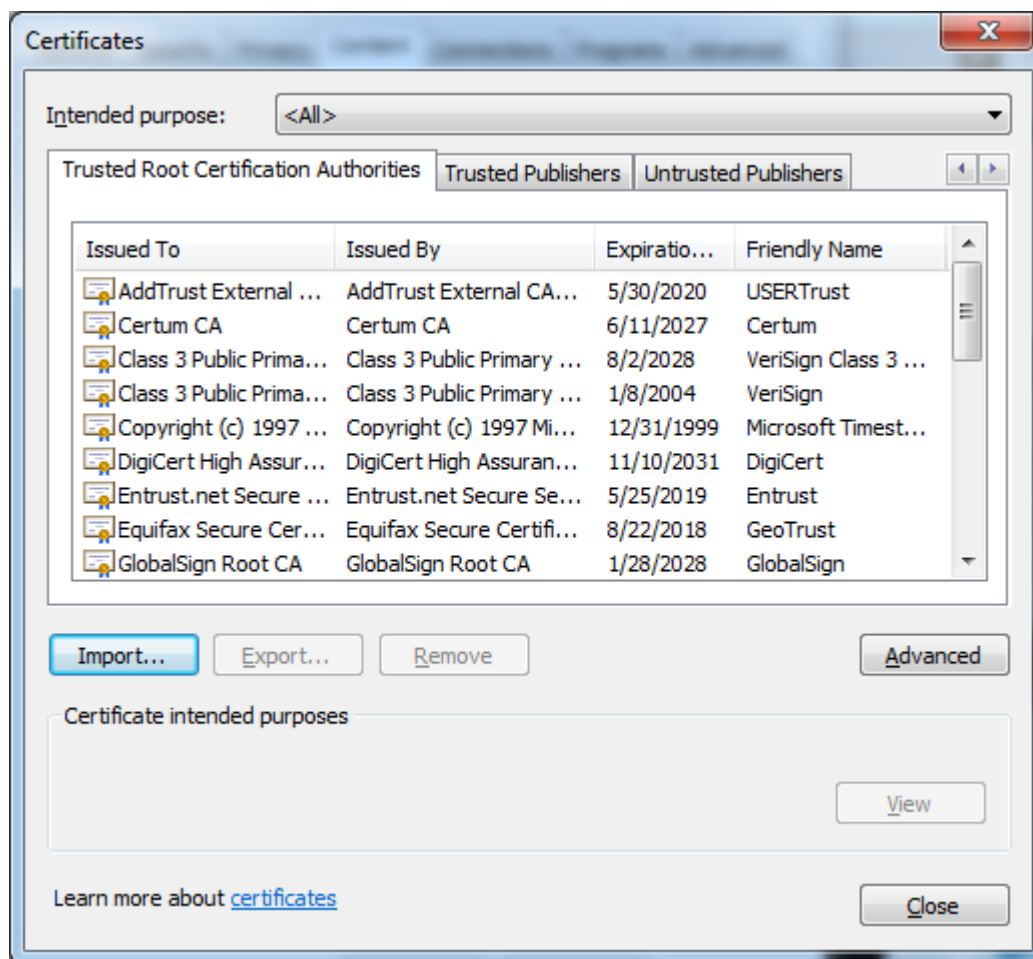
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

Another pop-up Certificate window will appear with three tabs namely "General", "Details" and "Certification Path".

Select the "General" tab and then click "Install Certificate..." button or go to Tools->Internet Options-> Content->Certificates.



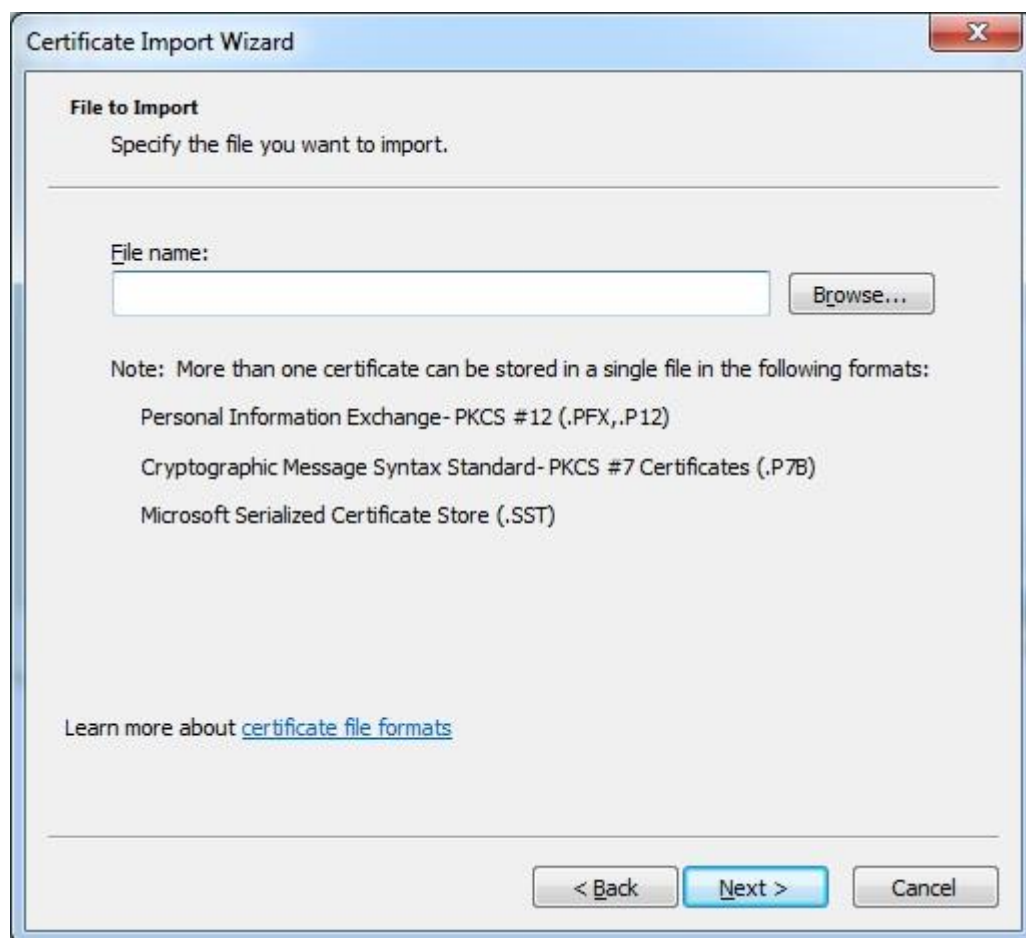
From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.



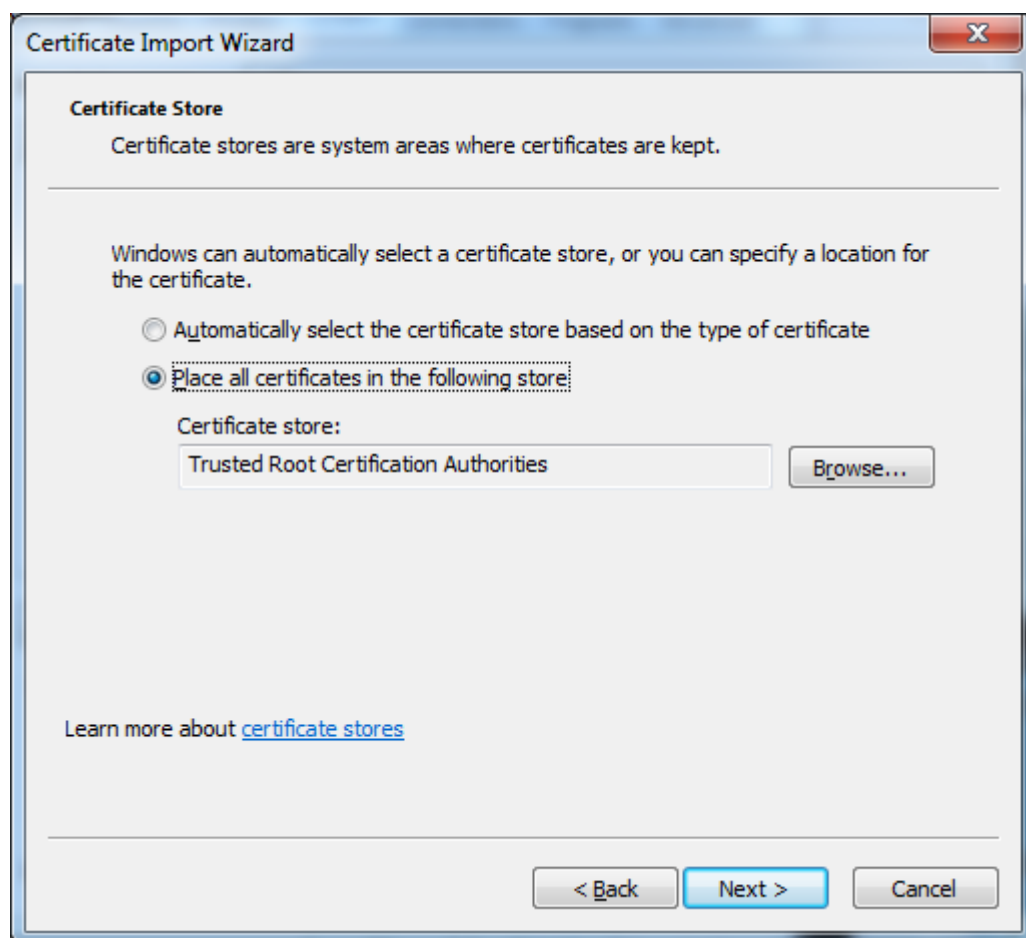
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.



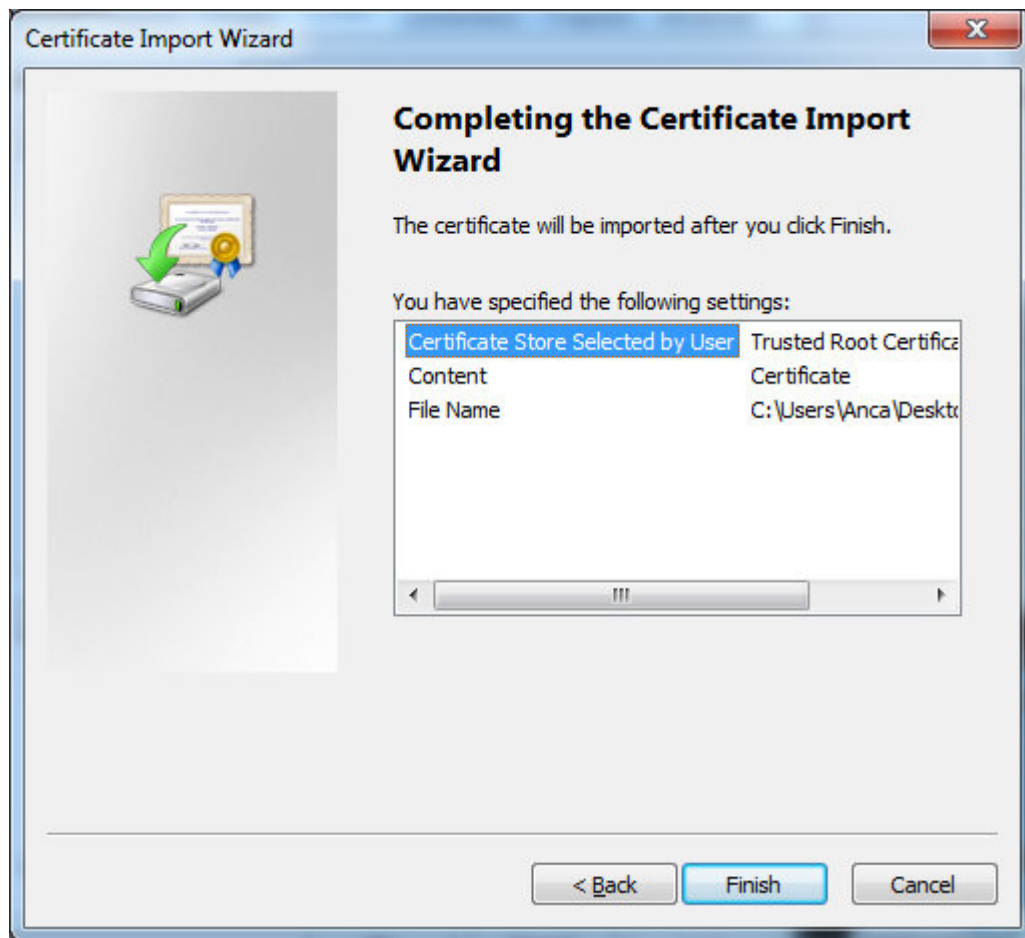
Browse for the Certificate file you downloaded from the Appliance Setup Wizard  
->Appliance Server Certificate.



In the Certificate Store window, select “Place all certificates in the following store” radio button.

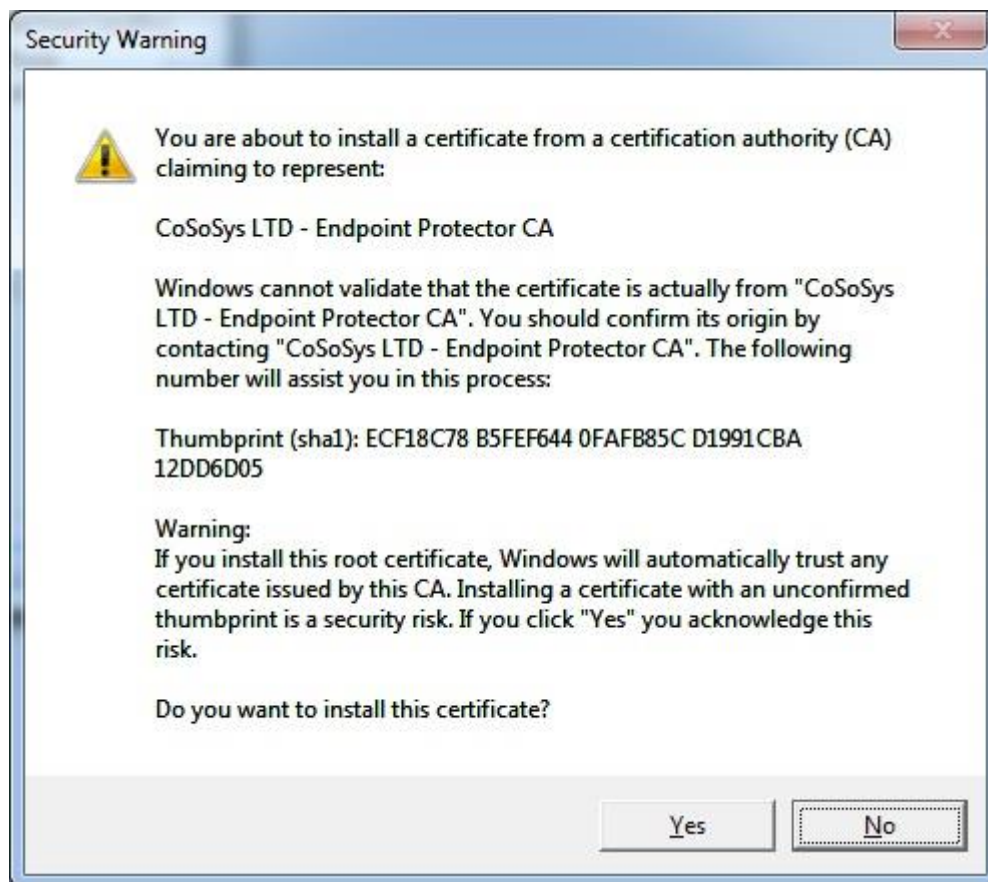


Another “Completing the Certificate Import Wizard” pops up. Just click the “Finish” button.



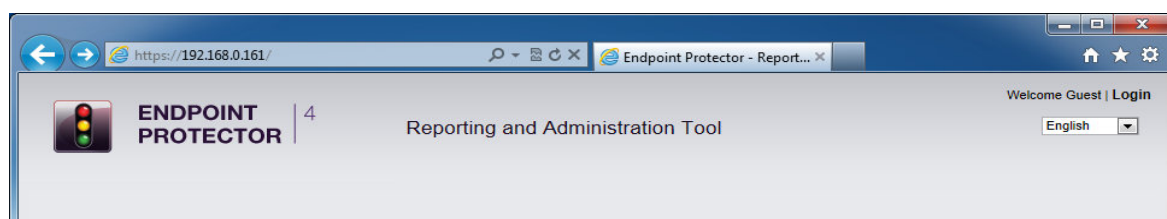


A Security Warning window pops up. Just click "Yes".



You have now successfully installed the Certificate.

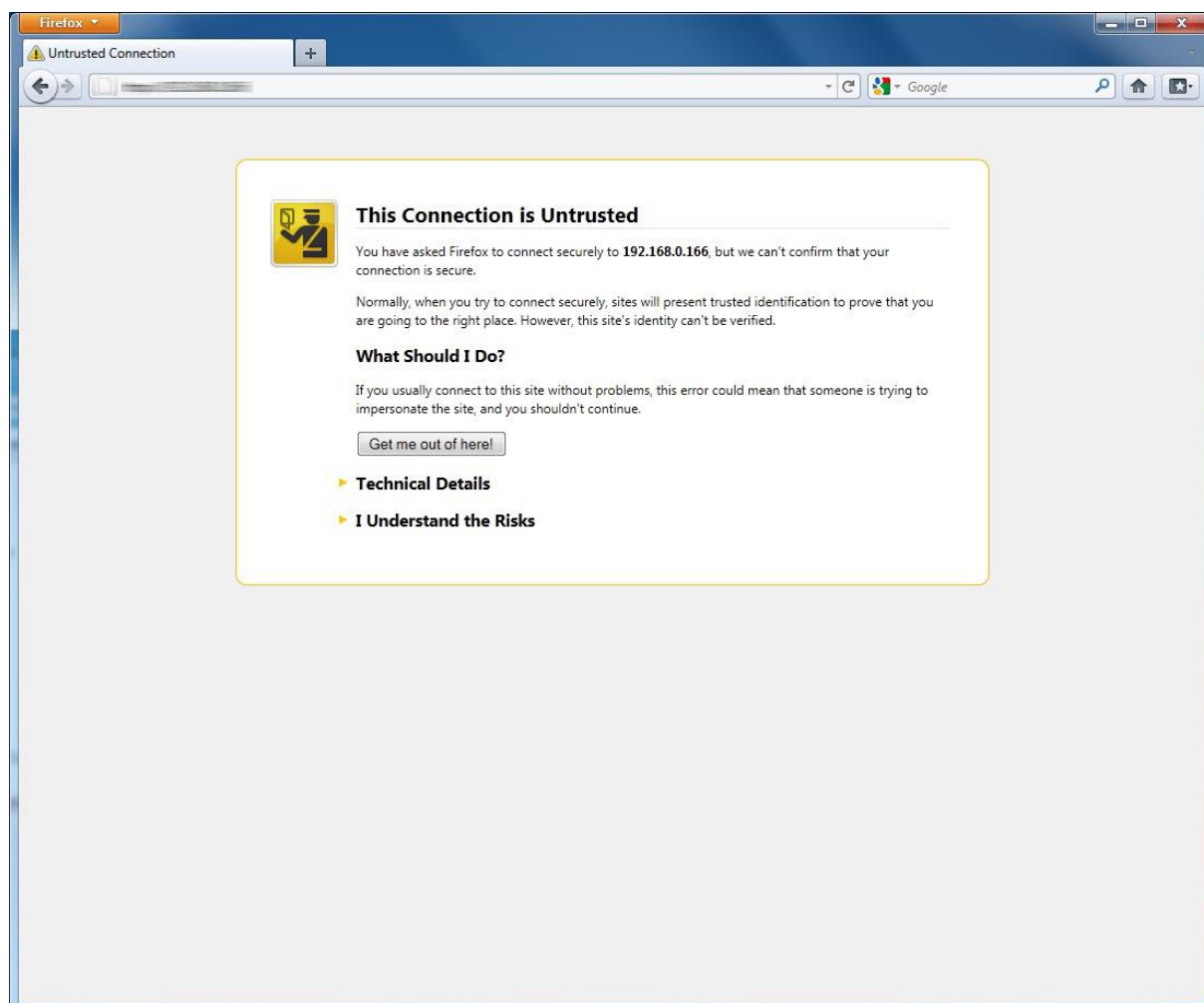
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



## 17.2. For Mozilla Firefox

Open the Browser.

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example <https://192.168.0.201>).



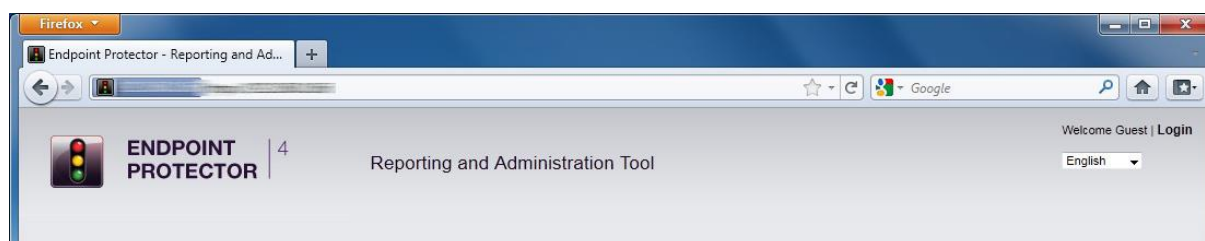
From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

Just click Get Certificate button and then the Confirm Security Exception button.



Close the browser and start it again.



# 18. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

## 18.1. Server Related

Appliance – Appliance refers to the Endpoint Protector Appliance which is running the Endpoint Protector Server, Operating System, Databases, etc.

Computers – refers to PC's, workstations, thin clients, notebooks which have Endpoint Protector Client installed.

Devices – refers to a list of known mobile devices, ranging from iPhones, iPads and MacBooks to Android Smartphones and tablets.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

Departments – an alternative way to Groups to organize main entities (devices, users or computers), which involves also the administrators of Endpoint Protector.

Mobile Device Management (MDM) – a set of software and services that allow organizations to closely monitor, manage and secure employees' mobile devices regardless of the different mobile service providers and mobile operating systems being used.

BYOD – acronym that stands for "Bring Your Own Device", which refers to the new trend adopted by employees to take their own personal devices to work and directly interface to the corporate network.

Apple APNs Certificate – stands for Apple Push Notification Service and it is a certificate signed by Apple that enables the management of iOS and OS X devices by IT Administrators using available MDM software

Provisioning – refers to the process of providing mobile device users with appropriate access to all necessary enterprise resources and enforcement of company policies.

Enrollment – for mobile devices, it refers to the setup process for enabling Mobile Device Management for a specific mobile phone or tablet.

## 18.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC's, Workstations and/or Notebooks which have Endpoint Protector Client installed and are currently running and are connected to the Endpoint Protector server.

Connected devices – are devices which are connected to online computers.

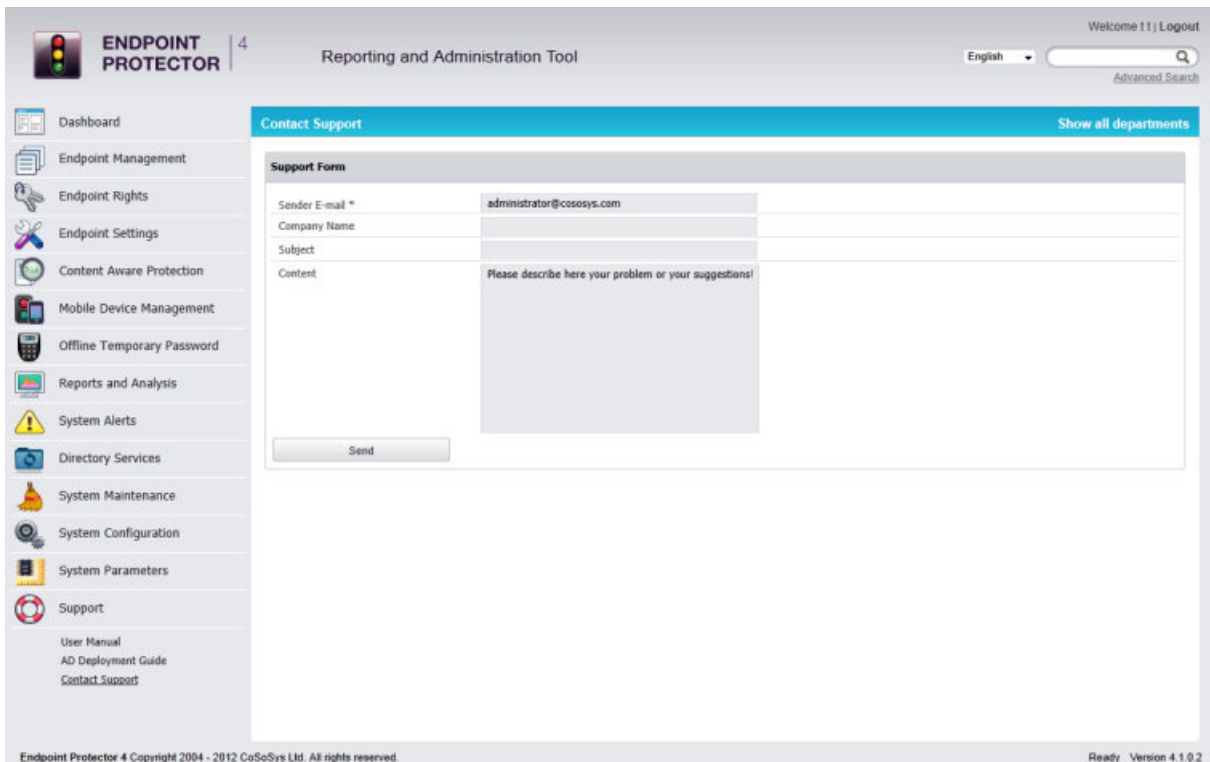
Events – are a list of actions that hold major significance in Endpoint Protector. There are currently 17 events that are monitored by Endpoint Protector:

- Connected – the action of connecting a device to a computer running Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File delete – a file located on a portable device has been deleted.

# 19. 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 displays the 'Endpoint Protector 4' Reporting and Administration Tool interface. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with a magnifying glass icon. A 'Welcome !!! Logout' link is visible in the top right corner. The left sidebar contains a list of navigation items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, System Maintenance, System Configuration, System Parameters, and Support. The 'Support' item is highlighted. Below the sidebar, the 'Contact Support' form is displayed. The form has a title bar 'Contact Support' with a 'Show all departments' link. The form fields include: 'Sender E-mail \*' (pre-filled with 'administrator@cososys.com'), 'Company Name', 'Subject', and 'Content' (with a placeholder text 'Please describe here your problem or your suggestions!'). A 'Send' button is located at the bottom left of the form. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2012 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.1.0.2'.

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.

# 20. 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 – 2014 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.