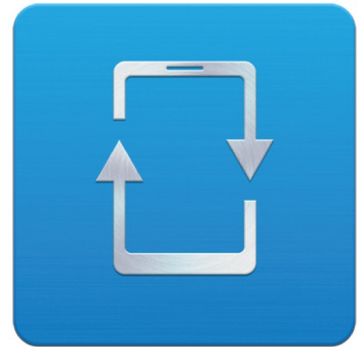


**COMODO**  
Creating Trust Online®



# Comodo Mobile Device Manager

Software Version 2.5

## Administrator Guide

Guide Version 2.5.111014

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Table of Contents

<b>1.Introduction to Comodo Mobile Device Manager.....</b>	<b>4</b>
1.1.Key Concepts.....	7
1.2.Best Practices.....	7
1.3.Quick Start.....	8
1.3.1.Using CMDM.....	9
<b>2.The Administrative Console.....</b>	<b>18</b>
2.1.Logging into your Administration Console.....	18
<b>3.The Dashboard.....</b>	<b>20</b>
<b>4.Managing Configuration Profiles and Apps.....</b>	<b>29</b>
4.1.Creating Configuration Profiles.....	30
4.1.1.Profiles for Android Devices.....	30
4.1.2.Profiles for iOS Devices.....	57
4.2.Viewing the Profiles.....	111
4.3.Editing Configuration Profiles.....	112
4.4.Managing Default Profiles.....	113
4.5.Managing Applications.....	118
<b>5.Managing Enrolled Devices and Users.....</b>	<b>125</b>
5.1.The Devices Interface.....	127
5.1.1.Managing an Individual Device.....	129
5.1.1.1.Viewing Summary Information.....	130
5.1.1.2.Viewing Hardware and Software Information.....	131
5.1.1.3.Managing Installed Applications.....	133
5.1.1.4.Managing Profiles Associated with the Device.....	134
5.1.1.5.Associating EAS Unknown Devices.....	136
5.1.2.Viewing the Location of the Device.....	137
5.1.3.Viewing the User Information.....	138
5.1.4.Removing a Device.....	139
5.1.5.Installing Apps on Devices.....	140
5.1.6.Generating Alarm on a Device.....	142
5.1.7.Locking/Unlocking Selected Devices.....	144
5.1.8.Configuring Access to Mailbox.....	146
5.1.9.Wiping Selected Devices.....	147
5.1.10.Assigning Configuration Profile to Selected Devices.....	148
5.1.11.Setting / Resetting Screen Lock Password for Selected Devices.....	150
5.1.12.Updating Device Information.....	152
5.1.13.Sending Text Message to Devices.....	153
5.2.Managing Device Groups.....	154
5.2.1.Creating Device Groups.....	156
5.2.2.Editing Device Groups.....	158
5.2.3.Assigning Configuration Profile to Groups.....	159
5.2.4.Removing a Device Group.....	161
5.3.Managing Users.....	161
5.3.1.Creating New Users and Enrolling their Devices.....	163
5.3.2.Adding Devices for Management.....	167

5.3.2.1.Enrolling Android Devices.....	168
5.3.2.2.Adding iOS Devices.....	174
5.3.2.3.Downloading and Installing CMDM Client for iOS Devices.....	177
5.3.3.Viewing the Details of a User.....	181
5.3.4.Updating the Details of a User and Resetting Password.....	181
5.3.5.Assigning Configuration Profile to a User.....	184
5.3.6.Adding Devices for Enrollment.....	186
5.3.7.Configuring User Access to Mailbox.....	187
5.3.8.Removing a User.....	189
5.4.Managing User Groups.....	189
5.4.1.Creating a New User Group.....	191
5.4.2.Editing a User Group.....	192
5.4.3.Assigning Configuration Profile to a User Group.....	194
5.4.4.Removing a User Group.....	194
5.5.Managing Applications on Enrolled Devices.....	195
5.5.1.Moving Selected Apps to Blacklist.....	197
5.5.2.Unblocking Blacklisted Apps.....	197
5.6.Managing Antivirus and Running Scans on Enrolled Devices.....	198
5.6.1.Running On-demand Antivirus Scans.....	200
5.6.2.Updating AV Databases on Devices.....	203
5.7.EAS Unknown Devices.....	204
<b>6.Reports.....</b>	<b>205</b>
6.1.Viewing Threats Reports.....	206
6.2.Viewing Event Logs from Individual Devices.....	207
6.3.Viewing User Activity Logs.....	210
<b>7.Configuring Comodo Mobile Device Manager.....</b>	<b>214</b>
7.1.Configuring Custom Variables.....	216
7.2.Configuring Email Templates.....	220
7.3.Adding Apple Push Notification Certificate.....	222
7.4.Configuring Google Cloud Messaging (GCM) for Android.....	225
7.5.Configuring the Android Agent.....	229
7.6.Configuring the Role-Based Access Control for Users.....	231
7.6.1.Creating a New Role.....	234
7.6.2.Managing Permissions and Assigned Users of a Role.....	236
7.6.3.Removing a Role.....	240
7.6.4.Managing Roles assigned to a User.....	241
7.7.Importing User Groups from LDAP.....	242
7.8.Antivirus Settings.....	247
7.9.Viewing and Managing Removed Devices.....	249
7.10.Viewing and Managing Licenses.....	249
7.10.1.Upgrading or Adding the License.....	250
7.11.Generating MDM Exchange Service Token.....	251
7.11.1.Installing Exchange Service.....	252
7.12.Viewing Version Information.....	256
<b>About Comodo.....</b>	<b>257</b>

# 1. Introduction to Comodo Mobile Device Manager

Comodo Mobile Device Manager (CMDM) allows administrators to manage, monitor and secure mobile devices which connect to their enterprise wireless networks.

Once a device has been enrolled, administrators can remotely apply configuration profiles which determine that device's network access rights, security settings and general preferences. CMDM also allows administrators to monitor the location of the device; run antivirus scans on the device; install/uninstall apps; remotely lock or wipe the device; view/start/stop running services; view reports on device hardware/software information; reset user passwords; make the device sound an alarm and more.



To enroll a device, administrators must first create a 'user'. Doing so will instruct CMDM to automatically send account activation and device enrollment mails to the user's email address. Both emails must be answered by the user on the device itself.

- The account activation mail contains a link which lets the user choose a unique password for logging in to the CMDM interface.
- The enrollment mail invites the user to download the CMDM app and, after installation, to enroll the device. Once enrolled, the device will be automatically assigned a default configuration profile. CMDM allows up to five device enrollments per user.

ID	Username	Email	Phone number	Last login	Time expired token	Count enroll left	Token status	Count devices	Mail Access
2970	helva	helva@gmail.com				0	Not Created	0	Allowed for user
2969	jack	jack@gmail.com				2	Active	0	Allowed for user
2968	Stewart	stewart@gmail.com		2014/05/14 01:27:09 PM	2014/05/17 12:37:43 PM	0	Active	0	Allowed for user
2967	robert	robert@gmail.com				1	Active	0	Allowed for user
2965	robert	robert@gmail.com		2014/05/14 11:22:28 AM	2014/05/17 01:24:24 PM	2	Active	3	Allowed for user
2963	robert	robert@gmail.com				2	Expired	1	Allowed for user
2962	robert	robert@gmail.com		2014/07/23 04:52:00 PM	2014/07/26 05:49:57 PM	1	Expired	0	Allowed for user
2961	robert	robert@gmail.com		2014/05/12 04:51:54 PM	2014/05/15 04:51:54 PM	0	Not Created	0	Allowed for user
2960	robert	robert@gmail.com	123456789	2014/07/23 12:07:20 PM	2014/07/26 04:32:03 PM	0	Expired	0	Allowed for user
2958	robert	robert@gmail.com	010203040506			0	Not Created	0	Allowed for user
2954	robert	robert@gmail.com	010203040506			0	Not Created	0	Allowed for user
2952	robert	robert@gmail.com	010203040506			0	Not Created	0	Allowed for user
2944	robert	robert@gmail.com	010203040506	2014/07/01 07:15:10 PM	2014/07/04 10:01:20 PM	0	Expired	0	Allowed for user
2937	robert	robert@gmail.com	010203040506	2014/07/04 05:47:13 PM	2014/07/04 10:01:20 PM	0	Expired	0	Allowed for user
2935	robert	robert@gmail.com	010203040506	2014/07/04 04:10:34 PM	2014/07/04 10:01:20 PM	0	Expired	0	Allowed for user
2921	robert	robert@gmail.com	010203040506	2014/07/04 05:50:20 PM	2014/07/04 10:01:20 PM	0	Expired	0	Allowed for user
2910	robert	robert@gmail.com	305-805-8104	2014/06/14 10:54:00 AM	2014/06/17 11:50:21 AM	1	Active	2	Allowed for user
2911	robert	robert@gmail.com	305-805-8104	2014/06/07 06:23:19 PM	2014/06/14 12:31:20 PM	0	Expired	2	Allowed for user
2912	robert	robert@gmail.com	305-805-8104	2014/06/07 11:53:21 AM	2014/06/14 12:31:20 PM	0	Expired	2	Allowed for user

A 'profile' is a collection of settings which can be applied to mobile devices that have been enrolled into CMDM. Profiles are split into iOS profiles and Android profiles. Once created, a profile can be applied to an individual device, to a group of devices and/or designated as a 'default' profile.

## Guide Structure

This guide is intended to take you through the configuration and use of Comodo Mobile Device Manager and is broken down into the following main sections.

**Introduction to Comodo Mobile Device Manager** – Contains a high level overview of the service and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide.

**The Administrative Console** - Contains an overview of the main interface of CMDM and guidance to navigate to different areas of the interface.

**The Dashboard** – Describes the Dashboard area of the interface that allows the administrator to view a snapshot summary of devices and their statuses as pie-charts.

**Managing Configuration Profiles and Apps** – Covers creation and management of configuration profiles to be applied to enrolled iOS and Android Smartphones and Tablets. Also covers management of applications that can be pushed to enrolled devices from the CMDM console.

- **Creating Configuration Profiles**
- **Viewing the Profiles**
- **Editing Configuration Profiles**
- **Managing Default Profiles**
- **Managing Applications**

**Managing Enrolled Devices and Users** – Covers creation and management of users, viewing details, management and control of enrolled Smartphones and Tablets, remotely generating sirens, wiping, locking and powering off enrolled devices, remotely installing and managing apps on devices, managing device groups and running AV scans.

- **The Devices Interface**
  - **Managing an Individual Device**
  - **Viewing the Location of the Device**
  - **Viewing the User Information**
  - **Removing a Device**
  - **Installing Apps on Devices**
  - **Generating Alarm on a Device**
  - **Locking/Unlocking Selected devices**
  - **Wiping Selected Devices**

- **Assigning Configuration Profile to Selected Devices**
- **Setting / Resetting Screen Lock Password for Selected Devices**
- **Updating Device Information**
- **Sending Text Messages to Devices**
- **Managing Device Groups**
  - **Creating Device Groups**
  - **Editing Device Groups**
  - **Assigning Configuration Profile to Groups**
- **Managing Users**
  - **Creating a New Users and Enrolling their Devices**
  - **Adding Devices for Management**
  - **Viewing the Details of a User**
  - **Updating the details of a User and Resetting Password**
  - **Assigning Configuration Profile to a User**
  - **Adding Devices for Enrollment**
  - **Removing a User**
- **Managing User Groups**
  - **Creating a New User Group**
  - **Editing a User Group**
  - **Assigning Configuration Profile to a User Group**
  - **Removing a User Group**
- **Managing Applications on Enrolled Devices**
  - **Moving Selected Apps to Blacklist**
  - **Unblocking Blacklisted Apps**
- **Managing Antivirus and Running Scans on Enrolled Devices**
  - **Running On-demand Antivirus Scan**
  - **Updating AV Databases on Devices**

**Reports** - Covers the CMDM reports that can be viewed by the administrator.

- **Viewing Threats Reports**
- **Viewing Event Logs from Individual Devices**
- **Viewing User Activity Logs**

**Configuring Comodo Mobile Device Manager** – Contains explanations and tutorials on creating admin and user roles with different privilege levels and appropriately assigning them to enrolled users and configuring the behavior of various CMDM components. Also covers management of subscriptions and renewal/upgrade of licenses.

- **Configuring Custom Variables**
- **Configuring Email Templates**
- **Adding Apple Push Notification Certificate**
- **Configuring Google Cloud Messaging (GCM) for Android**
- **Configuring the Android Agent**
- **Configuring the Role-Based Access Control for Users**
  - **Creating a New Role**
  - **Managing Permissions and Assigned Users of a Role**
  - **Removing a Role**
  - **Managing Roles assigned to a User**

- **Importing User Groups from LDAP**
- **Antivirus Settings**
- **Viewing and Managing Removed Devices**
- **Viewing and Managing Licenses**
  - **Upgrading or Renewing the License**
- **Generating MDM Exchange Service Token**
- **Viewing Version Information**

## 1.1. Key Concepts

**Mobile Device** – For the purposes of this guide, a mobile device is any Android or iOS smart phone or tablet that is allowed to connect to the enterprise network through a wireless connection. Comodo Mobile Device Manager allows network administrators to remotely configure device access rights, security settings, general preferences and to monitor and manage the device. Mobile devices may be employee or company owned.

**User** – An employee or guest of the enterprise whose mobile device(s) are managed by the CMDM console. A user can also log into the CMDM console to view dashboard statistics for their own device(s). Users must be created before their devices can be added.

**Device Group** – An administrator-defined grouping of either Android or iOS devices that allows administrators to apply configuration profile(s) to multiple devices at once.

**Quarantine** – If the antivirus scanner detects a malicious application on a device then it may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any infected files moved into quarantine are encrypted so they cannot run or be executed. The quarantine feature is only available for rooted devices.

**Configuration Profile** - A configuration profile is a collection of settings applied to enrolled device(s) which determine network access rights, overall security policy, antivirus scan schedule and other preferences. Profiles are split into iOS profiles and Android profiles. Profiles can be applied to an individual device, to a group of devices or designated as a 'default' profile.

**Default Profile** - Default profiles are immediately applied to a device when it is first enrolled into CMDM. Default profiles are split into two types – iOS default profiles and Android default profiles. Multiple default profiles can be created and applied to a device or group of devices.

**CMDM Agent** – The agent is an Android app which needs to be installed on all Android devices to facilitate communication with the CMDM server. The agent app is responsible for receiving and executing tasks such as implementing configuration profiles, fetching device details, running antivirus scans, adding or removing apps and to lock or wipe the device.

**Reports** - Reports allow administrators to view detailed information about enrolled devices and to quickly identify and troubleshoot any problems. For example, reports will tell an administrator which devices are compliant with their profiles, how many threats have been identified on the network and to view individual device logs.

**Notifications** – Notifications are sent to devices by CMDM after events like the installation or removal of an app or because a threat has been identified on the device.

## 1.2. Best Practices

1. Default profiles are automatically applied to a device when it is first enrolled. It is prudent, therefore, to keep them as simple as possible as you can always deploy more refined policies later. For example, you can set up passcode complexity and encryption profiles that will provide immediate, protection for enrolled devices. Default profiles will also be applied to devices when:
  - Currently active policies are removed
  - A device is removed from a device group

See **Managing Default Profiles** for more information.

2. Though it is possible to save all settings in a single profile, an option worth considering is to create separate profiles dedicated to the implementation of a single setting group (remember, many profiles can be applied at once to a device or group). For example, you could name a profile 'Android\_passcode\_profile' and configure only the passcode rules. You could create another called 'Android\_VPN\_settings' and so on. A system like this would allow you to construct bespoke profiles on-the-fly from a pool of known settings. Adding or removing a profile from a device would let you



quickly troubleshoot if a particular setting is causing issues.

See [Creating Configuration Profiles](#) for more details.

3. CMDM allows each user to enroll a maximum of five devices. However, administrators should initially keep this number at it's lowest workable level ('2' is a good starting point). While max. enrollments can be increased, they cannot be decreased. This is because administrators cannot de-enroll devices for a user. We encourage admins to evaluate the average number of devices per user and to set max. enrollments accordingly.

Refer to [Adding Devices for Enrollment](#) for more details.

4. Creating a group of devices is a great time-saver if the policies applied to them are going to be the same.

Refer to the section [Managing Device Groups](#) for more details.

5. The first level of defense on any device is to set a complex passcode policy. CMDM allows you specify passwords which are a combination of numbers, letters, special symbols and of a minimum length set by you. You can also set passcode lifetimes, reuse policy and define whether data should be automatically wiped after a certain number of failed logins.
6. Decide what restrictions are required for *your* company and *your* users. For example, disabling cell-phone cameras might be expected and mandatory in certain corporate environments but could be seen as a savage affront to liberties in more relaxed offices. CMDM offers flexible restrictions for Android devices over items such as Wi-Fi, packet data, bluetooth connectivity and use of camera. iOS restrictions are much more granular and also include App purchases, game center, voice dialing and more.

Refer to the restriction sections in [Profiles for Android Devices](#) and [Profiles for iOS Devices](#) for more details.

7. Keeps an eye on the apps you allow in your organization. Apps can be useful and productive to your employees but some may pose a malware or data-leak risk for your organization. CMDM provides you the ability to blacklist and whitelist apps, to govern how apps behave and to determine whether users are allowed to install apps from 3<sup>rd</sup> party vendors.

Refer to the section [Managing Applications on Enrolled Devices](#) for more details.

8. Keeping enrolled devices free from malware is vital to your organization's security. It is advisable to run antivirus scans on devices regularly per your company's needs. CMDM allows you to create a scheduled antivirus scan profile that automates the process of AV scans. If needed, AV scans can also be run instantly for selected devices or all enrolled devices.
9. CMDM interface can be accessed by users and the activities performed by them depends on the roles assigned to them. Privileges to users should be according to organizational hierarchy and requirements. CMDM allows to configure different roles with different privileges and assign them to users as per organizational needs. Refer to the section [Configuring the Role-Based Access Control for Users](#) for more details.
10. Check the devices statuses regularly for compliance of deployed profiles and other reports. CMDM provides at-a-glance view of platform details of devices, types of devices and other reports. Refer to the section [The Dashboard](#) and [Audit Reports](#) for more details.

## 1.3. Quick Start

This tutorial explains how an administrator can setup Comodo Mobile Device Manager (CMDM), login, add users, enroll devices, create device groups and create then deploy device configuration profiles.

Click any link to go straight to that section of your choice:

[Step 1 - Login to Admin Console](#)

[Step 2 – Add Users and Enroll Devices](#)

[Step 3 - Create Groups of devices](#) (Optional)

[Step 4 - Create Configuration Profiles](#)

[Step 5 - Apply profiles to devices or device groups](#)



## 1.3.1. Using CMDM

### Step 1 - Login to Admin Console

The Comodo Mobile Device Manager (CMDM) console can be viewed in any internet browser. CMDM is a locally hosted solution so, if you do not know the URL/hostname already, then please contact the administrator that installed the server.

The factory default username and password are:

Username: admin

Password: admin



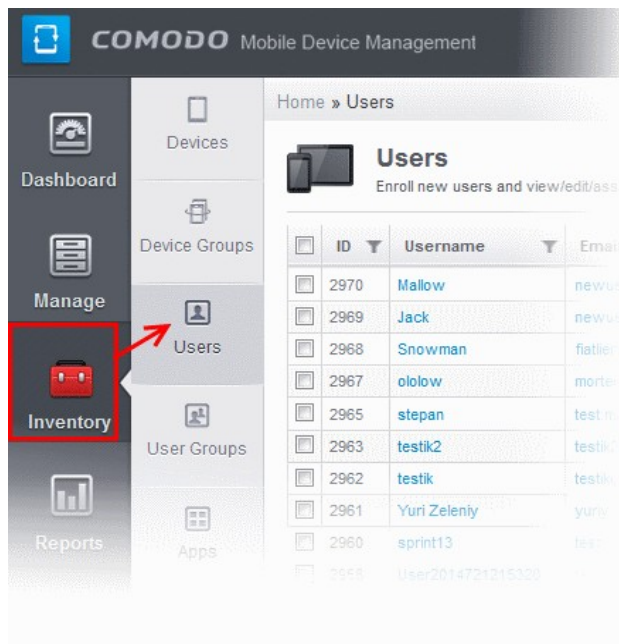
You can (and should) change these to a unique username and strong password. To do this, log in, click 'Inventory' > 'Users' then click on the user named 'Admin'. Next, click the 'Update' link. The 'Update User' screen will allow you to change your username and to initiate the reset password process.

### Step 2 – Add Users and Enroll Devices

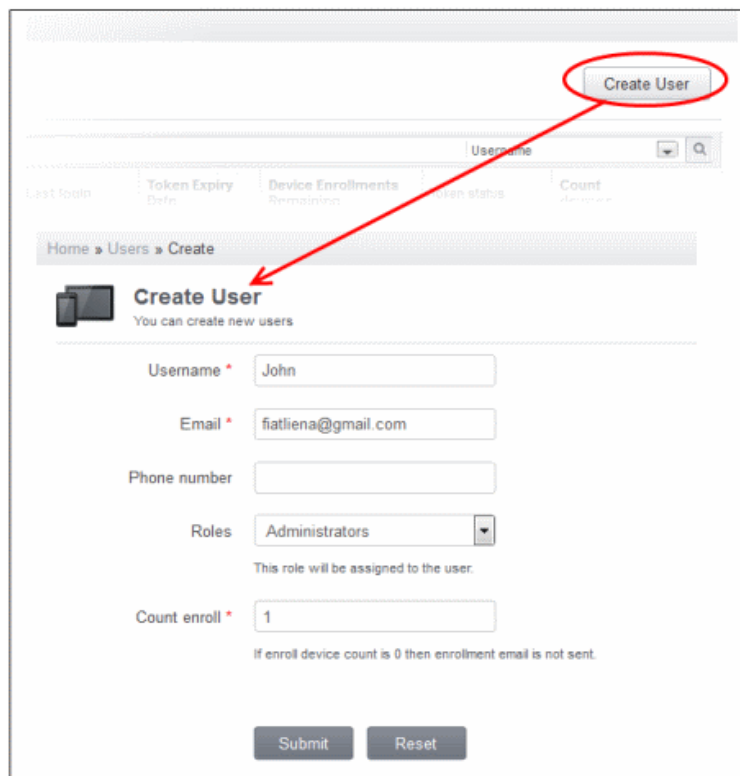
The first step in configuring CMDM is to add users. Immediately after adding a user, the system will send them two emails which need to be opened on the device itself. The first mail is so the user can set up and activate their account login. The second enables the user to enroll their device with the management system. The device enrollment process differs slightly between iOS and Android devices.

#### To add a new user

- Click the 'Inventory' tab from the left and choose 'Users'



- Next, click 'Create User' at the top right of the 'Users' interface:




- Type a login (mandatory), email address (mandatory), phone number and a role for the user.
- A 'role' determines user permissions within the CMDM console itself. CMDM ships with two default roles:
  - **Administrator** – Full administrative privileges in the CMDM console. The permissions for this role are not editable.
  - **User** – In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under CMDM factory settings, users can login to CMDM but can only view dashboard statistics for their own device.

You can create roles with different permission levels via the 'Role Management' screen (click 'Settings > Role Management'). You can edit the permissions of existing roles by clicking the magnifying glass at the end of the row followed by 'Actions > Edit'. Any new roles you create will become available for selection in the 'Roles' drop-down when creating a new user. See [Configuring the Role-Based Access Control for Users](#) and [Managing Roles assigned to a User](#) for more details.

- 'Count Enroll' determines how many devices a particular user is allowed to add. Each user can have a maximum of 5 devices. If you set this to zero, then the user will be added but the device enrollment mails will not be sent.
- Click 'Submit' to add the user to CMDM.

Home » Users » User Info: John

 **View User: John**

Update

ID	2591
Username	John
Email	<a href="mailto:fiatliena@gmail.com">fiatliena@gmail.com</a>
Phone number	
User created	2014/06/26 10:39:00 AM
Last login	Not set
Time expired token	2014/06/29 10:39:01 AM
Count enroll left	1
Token status	Active
Count devices	0
Change password time	1970/01/01 01:00:00 AM

As soon as a new user is created, CMDM will send them two emails - one for account activation and the other for device enrollment. Each mail should be answered by the user on the device itself. You can add up to five devices per user.

### Enroll Android Phones and Tablets

The device enrollment email contains two links. The first to download the Android app and the second to enroll the device:

1. User opens the email on the target device and clicks the 1st link to install the CMDM app.
2. After app installation is complete, user clicks the 2nd link to enroll their device. The app will connect to CMDM and then the user needs to tap 'Activate' in the next screen. The app will automatically enroll the device with CMDM.

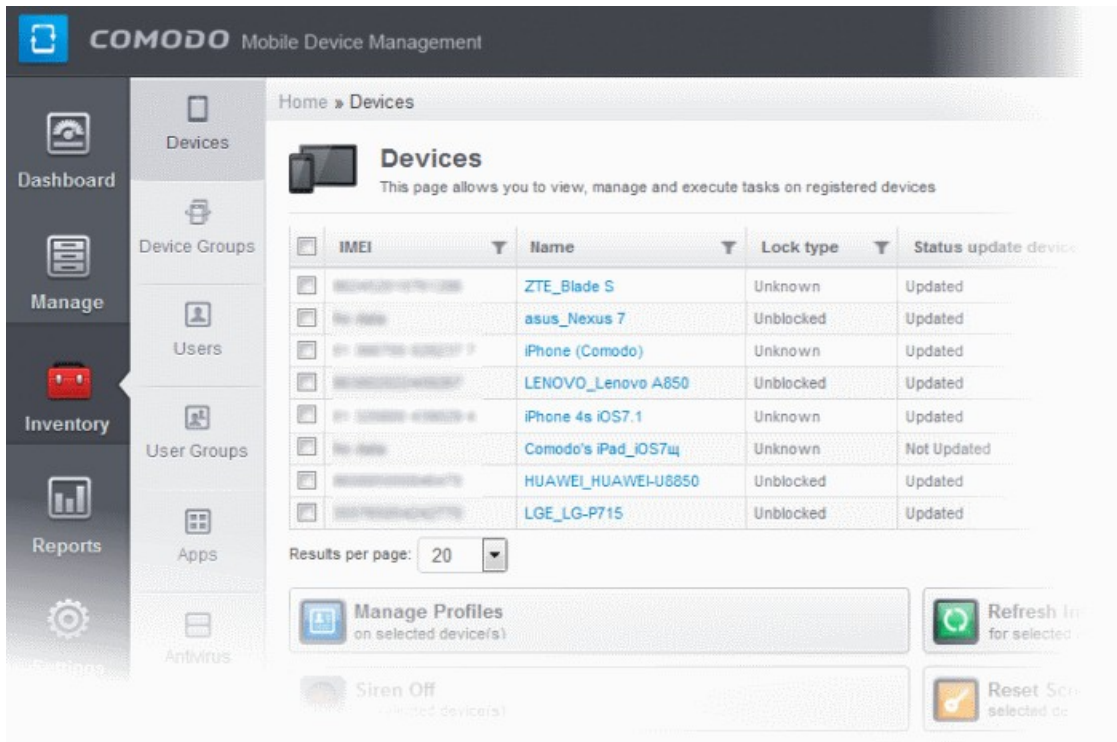
### Enroll iPhones, iPods and iPads

The device enrollment email contains a single enrollment link. The user clicks this link to download the CMDM client authentication certificate and CMDM profile. Once installed, the authentication certificate will be used to verify the user and the device when he or she attempts to connect to your network.

**Note:** The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

1. User receives enrollment mail, opens the device enroll link that automatically installs the certificate and CMDM profile on their device. This will enroll the device into CMDM.

The 'Devices' interface allows you to check that the device has been enrolled successfully:



The 'Devices' interface contains a list of all enrolled devices with columns that indicate the device IMEI, owner, platform and more. The bottom of the interface interface allows you to quickly perform remote tasks on selected devices, including device wipe/lock/unlock/shutdown, siren on/off, install apps and password set/reset.



See [The Devices Interface](#) for more details.

### Step 3 - Create Groups of Devices


Administrators can create groups of Android or iOS devices that will allow them to view, manage and apply policies to large numbers of devices. A group must either be an Android group or an iOS group. Beyond that, groups can be created according to administrator preference. Example groups could include 'Sales Department iPhones', 'Accounts Department Android Devices', 'All Android Tablets', 'iOS 7 iPads' and so on. Devices that are added to a particular group will automatically have the group security profiles applied to them. Devices can belong to more than one group and each group can have multiple profiles.

**To create a new group:**

- Click the 'Inventory' tab then select 'Devices Groups' to open the list of groups. Any existing groups will be shown here.
- Click either the 'Create Android device group' button or the 'Create iOS device group' button.
- The 'Create/Edit Device Group' interface will open. You now have to name the group and choose which devices you wish to add.
- Select the devices that you want to add to the group.

- Click 'Save'. Repeat the process to create more groups.
- Profiles are **explained in the next section**.

Home » Group devices » Create



### Create/Edit Device Group

Select devices to become members of a device group.

---

Group name \*

#### Step 4 - Create Configuration Profiles

A configuration profile is a collection of settings which can be applied to mobile devices that have been enrolled into Comodo Mobile Device Manager. Each profile allows an administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.

If you designate a profile as 'Default', then it will be auto-applied to a device upon enrollment. Multiple profiles can be created to cater to the different security and access requirements of devices connecting to your network.

Profiles are applied at the time a device connects to the network. Profile settings will remain in effect until such time as the CMDM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

Profile specification differs slightly between iOS and Android:

##### Android profiles

##### iOS profiles

#### To create Android Profiles

- Click the 'Manage' tab on the left and select 'Profiles'
- Click the 'Create Android profile' button at the bottom of the page
- Enter a name and description for the profile
- Select 'Default profile' if you wish this profile to be automatically applied to all newly enrolled Android devices.
- Click 'Save'.

Home » Profiles » Edit

## Edit Android Profile

**General**  
Configured

**Passcode**  
Not configured

**Restrictions**  
Not configured

**Anti-virus settings**  
Not configured

**Wi-Fi**  
Not configured

**Native App Restrictions**  
Not configured

**Email**  
Not configured

**VPN**  
Not configured

**Profile Name \***  
Password Profile

**Default profile**

**Description**

Fields with \* are required.

Save

### Android profile configuration screen

After saving, you will move onto profile configuration where you can configure passcode settings, feature restrictions, antivirus settings Wi-Fi settings and more. If a settings area is shown as 'Not Configured', then this profile will not apply any settings from that area. The device will continue to use existing, user-defined settings or settings that have been applied by another CMDM profile.

See [Profiles for Android Devices](#) in the full guide for more information on these settings. In brief:

- **General** – Profile name, description and whether or not this is a default profile. Default profiles are automatically applied upon device enrollment.
- **Passcode** - Specify passcode complexity, minimum length, timeout-before-lock, failed logins before wipe (0=unlimited/never wipe), maximum lifetime of passcode in days and number of previous passcodes from which the new passcode should be unique.
- **Restrictions** – Configure default device settings for Wi-Fi always-on, data-traffic on/off, whether users should be able to disable background traffic, bluetooth on/off, whether camera use is allowed when connected, whether the user is allowed to encrypt data stored on the device and whether or not they are allowed to install applications from unknown sources.
- **Antivirus Settings** – Schedule antivirus scans on the device and, if relevant to your setup, specify the location from which the agent should download virus database updates (leave this blank to collect updates from Comodo servers).
- **Wi-Fi** – Specify the name (SSID) and password (if required) of your wireless network. You also need to make sure 'Is enabled' is checked in order for your users to connect to the service. You can add other wireless networks by clicking 'Add new Wi-Fi section'.



- **Native App Restrictions** – Configure which native applications should be accessible to users. Native applications are those that ship with the device OS and include apps like Gmail, YouTube, the default Email client and the Gallery. This feature is supported for Android 4.0+ and Samsung for Enterprise (SAFE) devices such as Galaxy smartphones, Galaxy Note devices and Galaxy tablets.
- **Email** – Configure email account, connection and security details for users accessing incoming and outgoing mails from their devices. This profile is supported for SAFE devices only.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location. This profile is supported for SAFE devices only.
- **Kiosk** – Enable and configure Kiosk Mode for SAFE devices like the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices. This profile is supported for SAFE devices only.
- **Other Restrictions** – Configure a host of other permissions such as use of microphone, SD card, allow screen capture and more. This profile is supported for SAFE devices only.
- **Network Restrictions** – Specify network permissions such as minimum level of Wi-Fi security required to access that Wi-Fi network, allow user to add more Wi-Fi networks in their devices, type of text and multimedia messages to be allowed and configure whitelist/blacklisted Wi-Fi networks. This profile is supported for SAFE devices only.
- **Browser Restrictions** – Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- **Bluetooth Restrictions** – Specify Bluetooth restrictions such as to allow device discovery via Bluetooth, allow outgoing calls and more. This profile is supported for SAFE devices only.
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers. This profile is supported for SAFE devices only.

#### To create iOS Profiles

- Click the 'Manage' tab on the left and select 'Profiles' to open the 'Profiles list'.
- Click the 'Create iOS profile' button at the bottom of the interface.
- Enter a name and description for the profile (for example, 'iOS 7+ iPads' or 'Inside Sales Devices')
- Select 'Default profile' if you wish this profile to be automatically applied to all newly enrolled iOS devices.
- Messages typed in the 'Consent Text' box will be shown on the user's device when the profile is applied.
- Click 'Save'.

IOS device profiles are more detailed than Android profiles and contain **all the Android settings** plus the following areas:

**Airplay** – Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (iOS 7 +)

**Airprint** – Specify the location of Airprint printers so they can be reached by devices under this profile (iOS 7 +)

**VPN** – Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location.

**'Per-app' VPN** – Instead of forcing all BYOD traffic over the corporate VPN tunnel, 'Per-app VPN' functionality allows admins to choose specific 'managed apps' which should always connect via VPN. This improves user privacy and network performance by keeping all private browsing and emails off the corporate VPN. This section allows you to configure the VPN service that those managed apps will connect to.

**Mail** – Configure general mail server settings including incoming and outgoing servers, connection protocol (IMAP/POP), user-name/password and SMIME/SSL preferences.

**Exchange Active Sync** – Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.

**LDAP** – Configure LDAP account settings for devices under this profile so users can connect to company address books and contact lists.

**Calendar** – Configure CalDAV server and connection settings which will allow device integration with corporate scheduling and calendar services.

**Subscribed Calendars** – Specify one or more calendar services which you wish to push notifications to devices under

this profile.

**Contacts** – Configure CardDAV account, host and user-settings to enable contact synchronization between different address book providers (for example, to synchronize iOS contacts and Google contacts).

**Global HTTP Proxy** - Global HTTP proxies are used to ensure that all traffic going to and coming from an iOS device is routed through a specific proxy server. This, for example, allows the traffic to be packet-filtered regardless of the network that the user is connected through.

**Web Clip** – Allows you to push a shortcut to a website onto the home-screen of target devices. This section allows you to choose an icon, label and target URL for the web-clip.

**APN** – Specify an Access Point Name for devices on this profile. APN settings define the network path for all cellular data. This area allows you to configure a new APN name (GPRS access point), username/password and the address/port of the proxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.


**Cellulars Networks**– Configure cellular network settings. The 'cellulars' setting performs a similar role to the APN setting and actually replaces it in iOS 7 and above.

**Single Sign-On** – iOS 7 +. Configure user credentials that can be used to authenticate user permissions for multiple enterprise resources. This removes the need for a user to re-enter passwords. In this area, you will configure Kerberos principal name, realm and the URLs and apps that are permitted to use Kerberos credentials for authentication.

Click 'Save' button to store your new profile. See [Profiles for iOS Devices](#) in the main guide for more details on this area.

## Step 5 - Applying Profiles to Devices or Device Groups

### To apply a profile to specific devices

1. Click 'Inventory' > 'Devices', to open full list of currently enrolled devices.
2. Select the device(s) to which you wish to apply profile(s). Make sure all devices are of the same operating system (all iOS or all Android).
3. Click the 'Manage Profile' button  to open the profile selection and deployment screen.
4. The selected devices will be shown across the top of this page.

Devices **asus\_Nexus 7**

<input type="checkbox"/>	name
<input type="checkbox"/>	MikeMaxProfile
<input type="checkbox"/>	yuriy
<input type="checkbox"/>	E_Android
<input type="checkbox"/>	v_profiles
<input type="checkbox"/>	forTesting
<input type="checkbox"/>	--2
<input type="checkbox"/>	CoolWiFi
<input type="checkbox"/>	dev
<input checked="" type="checkbox"/>	test1
<input type="checkbox"/>	-----
<input type="checkbox"/>	K_Android profile
<input type="checkbox"/>	Demo profile
<input type="checkbox"/>	demo_profile
<input type="checkbox"/>	New Android Profile for demo
<input type="checkbox"/>	Demo Profile for teachers
<input type="checkbox"/>	v2_profiles
<input checked="" type="checkbox"/>	I_Default Profile
<input type="checkbox"/>	Maintenance Dept
<input type="checkbox"/>	Profile_password

**Save**

- To add a profile to the chosen device(s), select the check box(es) beside the profile.
- Click 'Save' for your changes to take effect. The selected profiles will be pushed to the chosen devices with immediate effect.

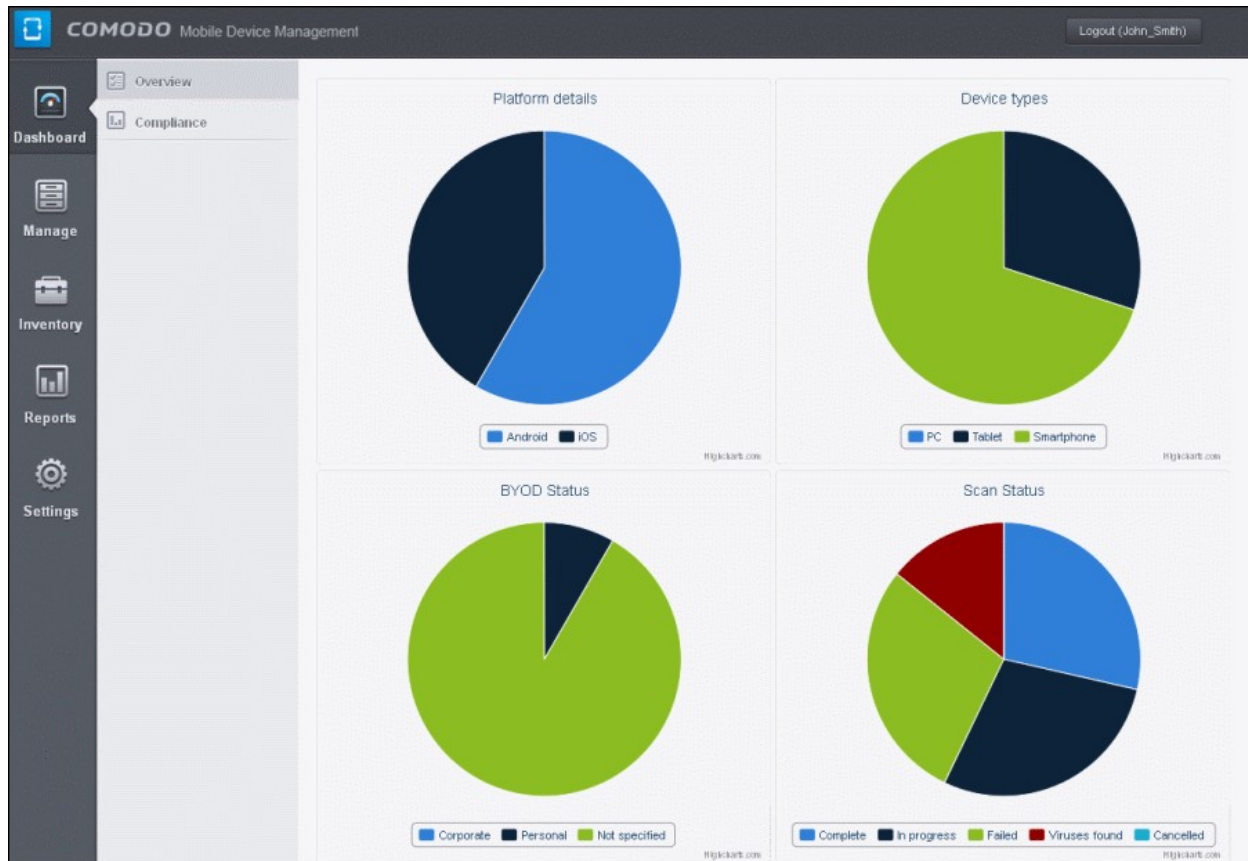
#### To apply profiles to a *group* of devices

- Click the 'Inventory' tab and choose 'Devices Groups' from the left hand menu
- Repeat bullets 2 – 5 of 'To apply a profile to specific devices'

If you have successfully followed all 6 steps of this quick start guide then you should have a created a basic working environment from which more detailed strategies can be developed. Should you need further assistance, each topic is covered in more granular detail in the full administrator guide. If you have problems that you feel have not been addressed, then please contact [mdmsupport@comodo.com](mailto:mdmsupport@comodo.com)

## 2. The Administrative Console

The Administrative Console is the nerve center of Comodo Mobile Device Manager (CMDM), allowing administrators to add users, enroll devices, create groups of devices, apply configuration profiles, run Antivirus (AV) scans and more.



Once logged-in, the administrator can navigate to different areas of the console by clicking the tabs at the left hand side.

**Dashboard** – Allows administrator to view snapshot summaries of details like operating systems, device types, AV scan status, Compliance status of devices enrolled to CMDM as pie-charts. See [The Dashboard](#) for more details.

**Manage** - Allows administrator to create configuration profiles to be applied to enrolled devices and groups of devices and to manage apps that can be pushed to enrolled devices from CMDM. See [Managing Configuration Profiles and Apps](#) for more details.

**Inventory** - Allows administrator to add and manage users to CMDM, manage and remotely control enrolled devices, create device groups for easy management, manage apps installed on selected devices and remotely install new applications and launch AV scans. See [Managing Enrolld Devices and Users](#) for more details.

**Reports** - Allows administrator to generate and view reports on viruses identified by AV scans, logs of devices and logs of user activities. Refer to the section [Reports](#) for more details.

**Settings** - Allows administrator to create admin and user roles with different privilege levels and appropriately assign them to users, configure the behavior of various CMDM components, and renew/upgrade licenses. See [Configuring Comodo Mobile Device Manager](#) for more details.

### 2.1. Logging into your Administration Console

Upon successful subscription of the service, the administrator will receive an account activation email containing the username and the activation link. The administrator can click the link to activate the account and set a password. Once activated, the administrator can login to the web based CMDM application using any Internet browser, by entering the URL of the CMDM interface. Comodo Mobile Device Manager is a locally hosted solution. If you do not know the URL of the admin login page, then please contact the personnel that installed the server.



- Enter your username and password and click Login.

**Important Note:** Password is case sensitive. Please make sure that you are entering it in proper case and Caps Lock is set OFF.

If you have forgotten your password, click the 'I forgot my password' link below the Login button. In the 'Password recovery' page, complete the procedure. A mail will be sent to your registered email id, where by clicking the 'Reset password' link you can reset a new a password.

After successful login, a 'Welcome to Comodo Mobile Device Management' screen will be displayed.



**Welcome to Comodo Mobile Device Management**  
Start to manage devices with a few simple steps.

- Create User**  
Go to [Inventory > Users](#) and click on "Create User" button
- Enroll your device**  
Open the email from Comodo MDM on your device and click on link.
- Configure the profile**  
Go to [Manage > Profiles](#). Click on profile name link and configure.
- Associate the profile with device**  
Go to [Inventory > Devices](#). Choose the device and press "Manage profiles" button.

The interface allows you to enroll users and start managing devices in a few steps:

- **Create User** – Allows you to add new users. Click the link [Inventory > Users](#) to add new users. Refer to the section [Creating New Users and Enrolling their Devices](#) for more details.
- **Enroll your device** – Allows you to enroll users' devices for managing. Refer to the section [Creating New Users and Enrolling their Devices](#) for more details.
- **Configure the profile** – Allows you to create and manage configuration profiles for both Android and iOS devices. Refer to the section [Managing Configuration Profiles and Apps](#) for more details.
- **Associate the profile with device** – Allows you to deploy and manage configuration profiles on devices. Refer to the section [Managing Enrolled Devices and Users](#) for more details.

## 3. The Dashboard

The Dashboard displays a snapshot summary of devices enrolled to Comodo Mobile Device Manager (CMDM), their types, ownership, Antivirus (AV) scan status and Compliance status of devices, as pie charts.

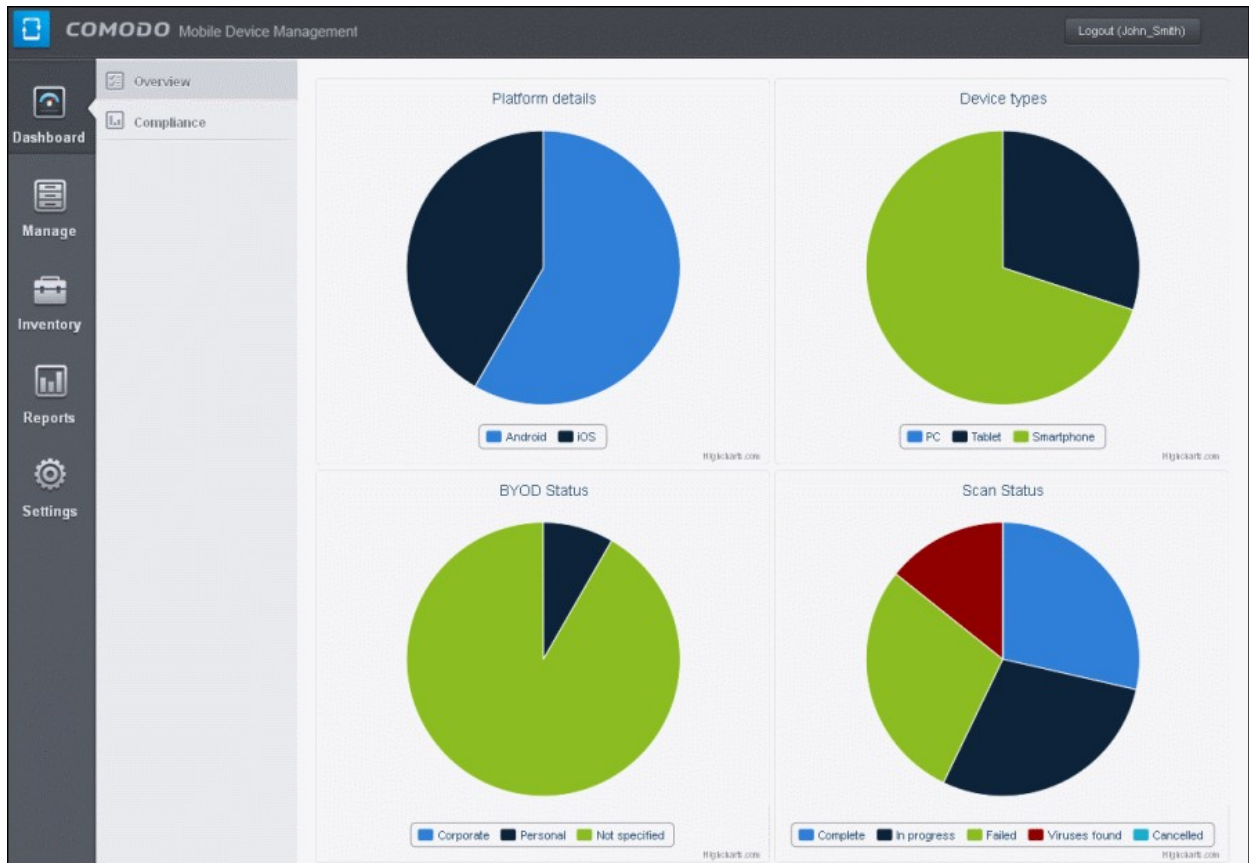
To open the 'Dashboard', click the Dashboard tab from the left hand side. It is divided into two sections, Overview and Compliance. Click the following links for more details:

- [Overview](#)
- [Compliance](#)

### Overview

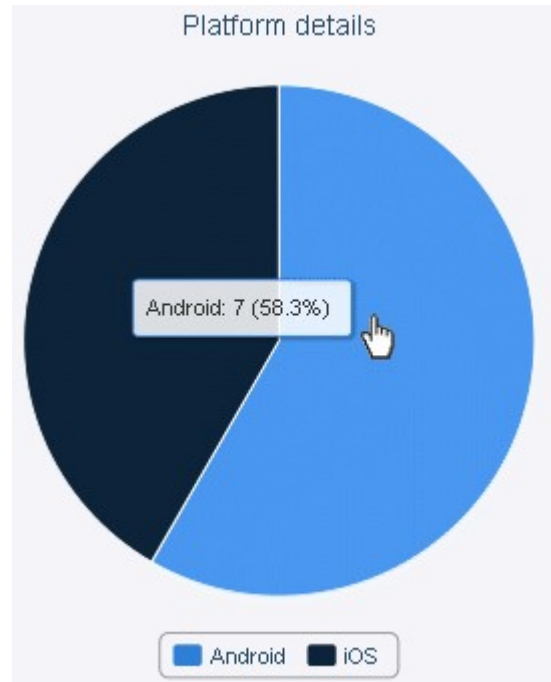
The overview screen provides a snapshot summary of devices enrolled to Comodo Mobile Device Manager (CMDM), their types, ownership, Antivirus (AV) scan status as pie charts.

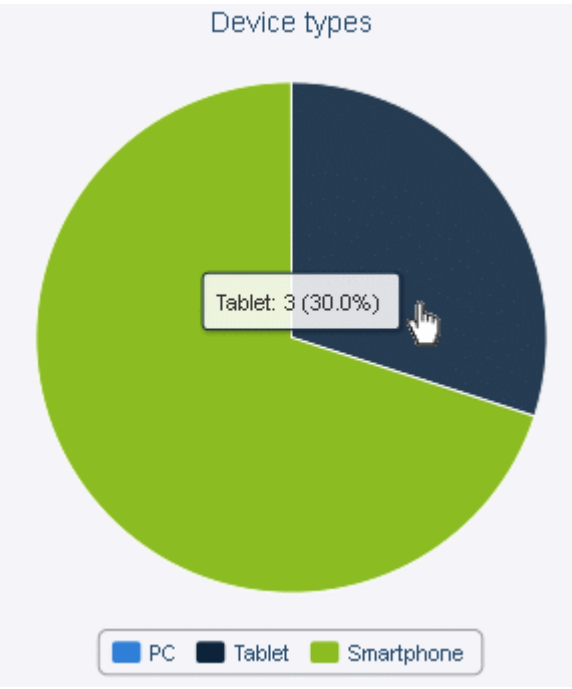
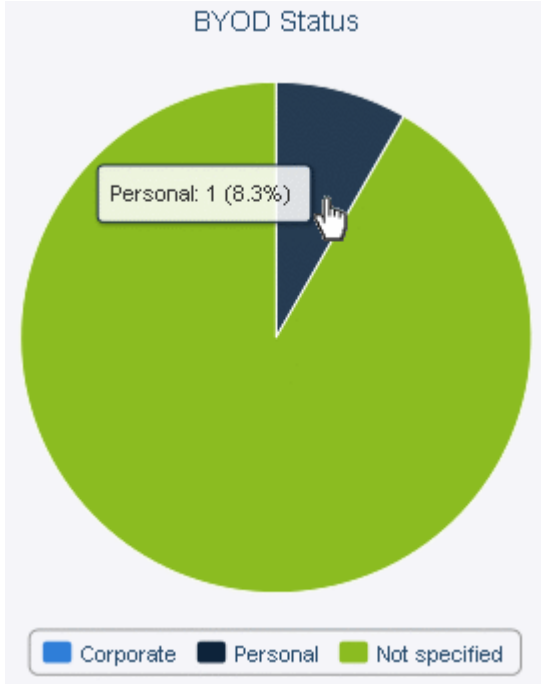


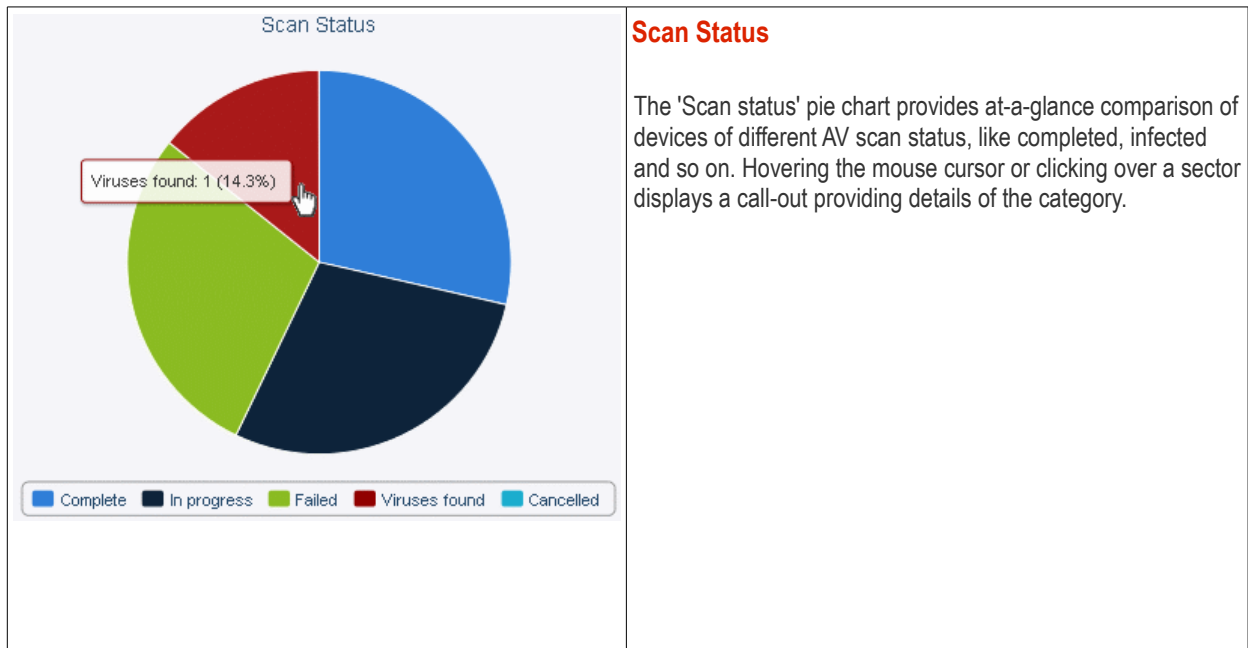


## Platform Details

The 'Platform details' pie chart provides at-a-glance comparison of devices of different Operating Systems. Hovering the mouse cursor or clicking over a sector displays a call-out providing details of the category.



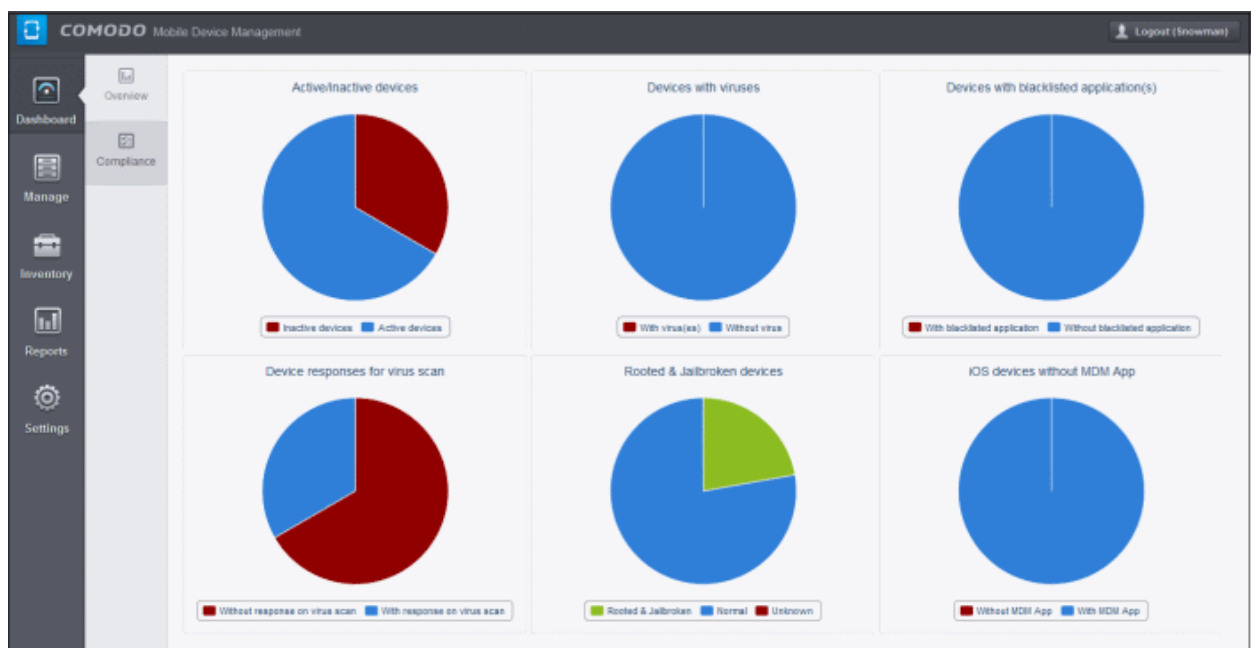
<p style="text-align: center;">Device types</p> 	<p><b>Device Types</b></p> <p>The 'Device Types' pie chart provides at-a-glance comparison of devices of different types like smart phones and tablets. Hovering the mouse cursor or clicking over a sector displays a call-out providing details of the category.</p>
<p><b>BYOD Status</b></p> <p>The 'BYOD summary' pie chart provides at-a-glance comparison of ownership of enrolled devices, like personal devices of the users, company owned devices lent to the users and so on. Hovering the mouse cursor or clicking over a sector displays a call-out providing details of the category.</p>	<p style="text-align: center;">BYOD Status</p> 



## Compliance

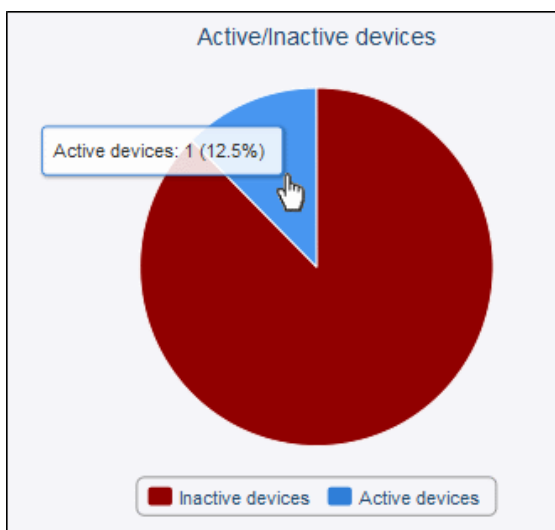
The compliance report of devices is a graphical summary of devices that are complaint and non-complaint, viruses status in the devices, blacklisted applications status and virus scan status in the enrolled devices.

To view the complaint status of the devices, click 'Dashboard' in the left side navigation and then 'Compliance'.



## Compliance Active / Inactive Devices

It is the summary of connectivity status of enrolled devices to CMDM. In CMDM, devices that are not connected for more than 20 minutes will be marked as inactive devices. Hovering the mouse cursor over a sector displays a call-out providing details of the category.



Clicking on any of the device status in the pie chart will open the respective 'Devices' page. For example, clicking on the 'Active devices' portion in the pie chart will open the 'Devices' page displaying the list of active devices.

Home » Devices

### Devices

List of active devices.

IMEI	Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Fail association	Mail Access
352638051036466	Sony Ericsson_WT19i	Unknown	Updated	Android	Snowman	2014/08/18 09:37:09 AM	27%	Successful	Allowed for device

Results per page: 20 Displaying 1-1 of 1 result

**Manage Profiles**  
(on selected device(s))

**Screen Off**

**Refresh Information**  
for selected device(s)

**Reset Screen-Lock Passcode**  
selected device(s)

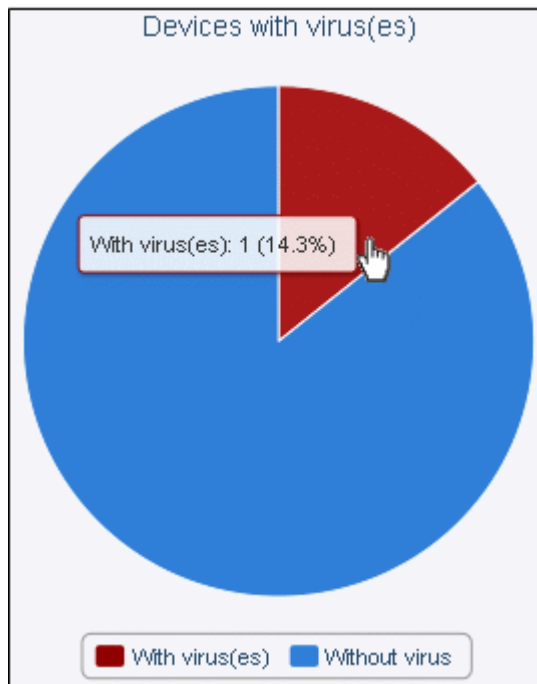
**Lock**  
on selected device(s)

**Deny access to mailbox**  
on selected device(s)

Similarly clicking on the 'Inactive devices' portion in the pie chart will open the 'Devices' page displaying the list of inactive devices. The devices screens allow you to manage the enrolled devices. Refer to the section **Managing Enrolled Devices** for more details.

## Devices With Viruses

The pie chart displays the status of enrolled devices that are affected and not affected by viruses after a virus scan. Hovering the mouse cursor over a sector displays a call-out providing details of the category. Refer to the section **Managing Antivirus and Running Scans on Enrolled Devices** for details about scanning for viruses on enrolled devices.



Clicking on any of the device status in the pie chart will open the respective 'AV Scan' page. For example, clicking on the 'Without viruses' portion in the pie chart will open the 'AV Scan' page displaying the list of devices without viruses.

Home » AV Scan

**Antivirus** Antivirus Settings  
List of devices without virus

<input type="checkbox"/>	Name	Device owner	Device type	OS	Last virus scan time	Malware detection status	Last scan
<input type="checkbox"/>	ZTE_Blade S		Smartphone		2014/08/15 05:35:00 PM	Clean	✔ Complete
<input type="checkbox"/>	LENOVO_Lenovo A850		Smartphone		2014/08/14 04:58:23 PM	Unknown	✘ Scan canceled
<input type="checkbox"/>	Sony Ericsson_WT19t	Snowman	Smartphone		2014/08/18 09:21:14 AM	Unknown	⌚ Scanning
<input type="checkbox"/>	HUAWEI_HUAWEI-U8850		Smartphone		Never	Unknown	Unknown
<input type="checkbox"/>	LGE_LG-P715		Smartphone		2014/07/28 03:49:22 PM	Clean	✔ Complete

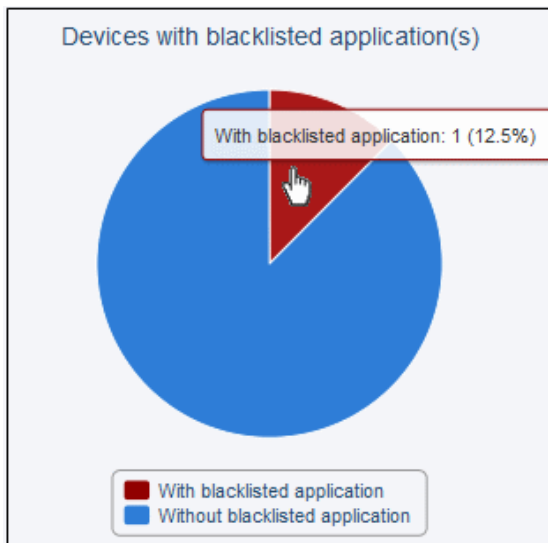
Results per page: 20 Displaying 1-5 of 5 results.

Quick Scan

The AV Scan Devices page allows you to run antivirus scan, updated AV database and more. Refer to the section **Managing Antivirus and Running Scans on Enrolled Devices** for more details.

### Devices with Blacklisted Application(s)

The pie chart displays the status of enrolled devices that have and do not have blacklisted applications in them. Hovering the mouse cursor over a sector displays a call-out providing details of the category. Refer to the section **Managing Applications on Enrolled Devices** for details about adding and removing apps from blacklist.



Clicking on any of the device status in the pie chart will open the respective 'Devices' page. For example, clicking on the 'With blacklisted application' portion in the pie chart will open the 'Devices' page displaying the list of devices with applications that are blacklisted.

Home » Devices

### Devices

List of devices that have blacklisted applications

IMEI	Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Fail association	Mail Access
352638051036466	Sony Ericsson_WT19i	Unknown	Updated	Android	Snowman	2014/08/18 10:07:14 AM	65%	Successful	Allowed for device

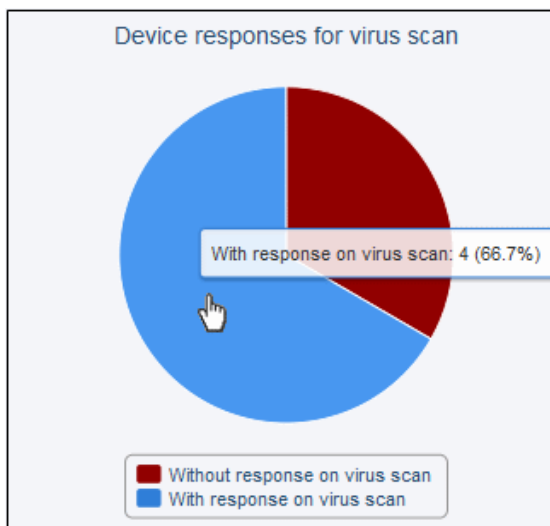
Results per page: 20 | Displaying 1-1 of 1 result

The devices screens allow you to manage the enrolled devices. Refer to the section **Managing Enrolled Devices** for more details.

### Device Response for Virus Scan

The pie chart displays the status of enrolled devices that are responding and not responding to virus scan. Hovering the mouse cursor over a sector displays a call-out providing details of the category. Refer to the section **Managing Antivirus and Running Scans on Enrolled Devices** for details about scanning for viruses on enrolled devices.





Clicking on any of the device status in the pie chart will open the respective 'AV Scan' page. For example, clicking on the 'With response on virus scan' portion in the pie chart will open the 'AV Scan' page displaying the list of devices that are responding to scan command.

Home » AV Scan

### Antivirus

List of devices that scan is completed [Antivirus Settings](#)

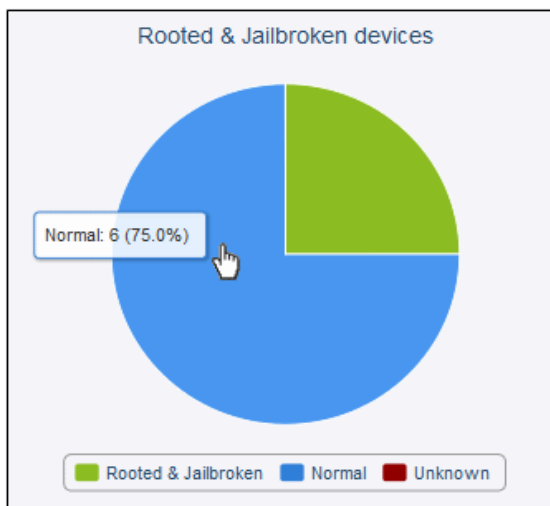
Name	Device owner	Device type	OS	Last virus scan time	Malware detection status	Last scan
ZTE_Blade S	[Avatar]	Smartphone	[Android Icon]	2014/08/15 05:35:00 PM	Clean	Complete
asus_Nexus 7	[Avatar]	Tablet	[Android Icon]	2014/08/15 05:48:31 PM	Infected	Viruses Found
LENOVO_Lenovo A850	[Avatar]	Smartphone	[Android Icon]	2014/08/14 04:58:23 PM	Unknown	Scan canceled
LGE_LG-P715	[Avatar]	Smartphone	[Android Icon]	2014/07/28 03:49:22 PM	Clean	Complete

Results per page: 20 Displaying 1-4 of 4 results

The AV Scan page allows you to run antivirus scan, updated AV database and more. Refer to the section **Managing Antivirus and Running Scans on Enrolled Devices** for more details.

### Rooted & Jailbroken Devices

The pie chart displays the number and percentage of enrolled devices that are rooted, jailbroken, normal and unknown in CMDM. Placing the mouse cursor over a sector displays a call-out providing details of the category.



Clicking on any of the status in the pie chart will open the respective 'Devices' page. For example, clicking on the 'Normal' portion in the pie chart will open the 'Device' page displaying the list of devices that are normal devices, that is, not rooted or jailbroken devices.

Home » Devices

### Devices

List of not rooted (normal) devices.

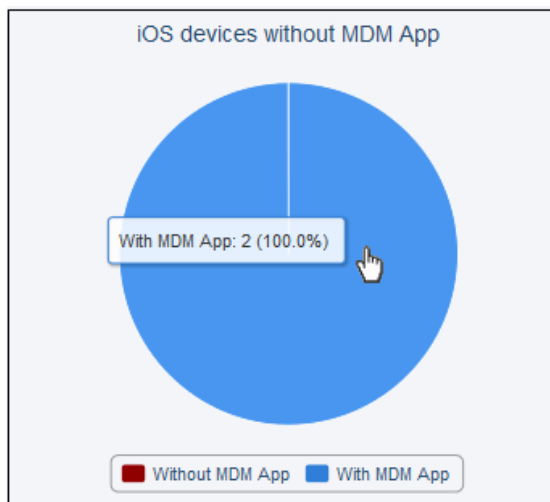
IMEI	Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Fail association	Mail Access
0000000000000000	iPhone 4s(Comodo)	Unknown	Not Updated	iOS	Comodo	2014/08/17 02:25:33 PM	30%	✓ Successful	Allowed for device
0000000000000000	iPhone 4s iOS7.1	Unknown	Not Updated	iOS	Comodo	2014/08/17 02:25:59 PM	25%	✓ Successful	Allowed for device
0000000000000000	asus_Nexus 7	Unblocked	Updated	Android	Comodo	2014/08/17 10:41:28 AM	15%	✓ Successful	Allowed for device
0000000000000000	LENOVO_Lenovo A850	Unblocked	Updated	Android	Comodo	2014/08/14 11:23:32 PM	33%	✓ Successful	Allowed for device
0000000000000000	Sony Ericsson_WT19i	Unknown	Updated	Symbian	Snowman	2014/08/18 10:27:47 AM	84%	✓ Successful	Allowed for device
0000000000000000	HUAWEI_HUAWEI-U8850	Unblocked	Updated	Android	Comodo	2014/07/25 04:39:33 PM	5%	✓ Successful	Allowed for device

Results per page: 20 | Displaying 1-6 of 6 results

Siren Off | Device Management Tools | Help

## iOS Devices Without MDM App

The pie chart displays the number and percentage of enrolled devices that have MDM app. iOS devices communicate with CMDM server via the MDM profile that was installed during enrollment and do not require MDM app. Installing MDM app helps to enhance the functionality such as getting location details of the device, sending messages from the admin panel and so on. Placing the mouse cursor over a sector displays a call-out providing details of the category.



Clicking on any of the status in the pie chart will open the respective 'Devices' page. For example, clicking on the 'With MDM App' portion in the pie chart will open the 'Device' page displaying the list of devices that have MDM app.

Home » Devices

**Devices**  
List of devices with MDM application installed.

IMEI	Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Fail association	Mail Access
	Phone 4s(Comodo)	Unknown	Not Updated	iOS		2014/08/17 02:25:33 PM	30%	✓ Successful	Allowed for device ✗
	Phone 4s iOS7.1	Unknown	Not Updated	iOS		2014/08/17 02:25:58 PM	25%	✓ Successful	Allowed for device ✗

Results per page: 20 Displaying 1-2 of 2 results

**Manage Profiles**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Reset Screen-Lock Passcode**  
selected device(s)

**Lock**  
on selected device(s)

**Deny access to mailbox**  
on selected device(s)

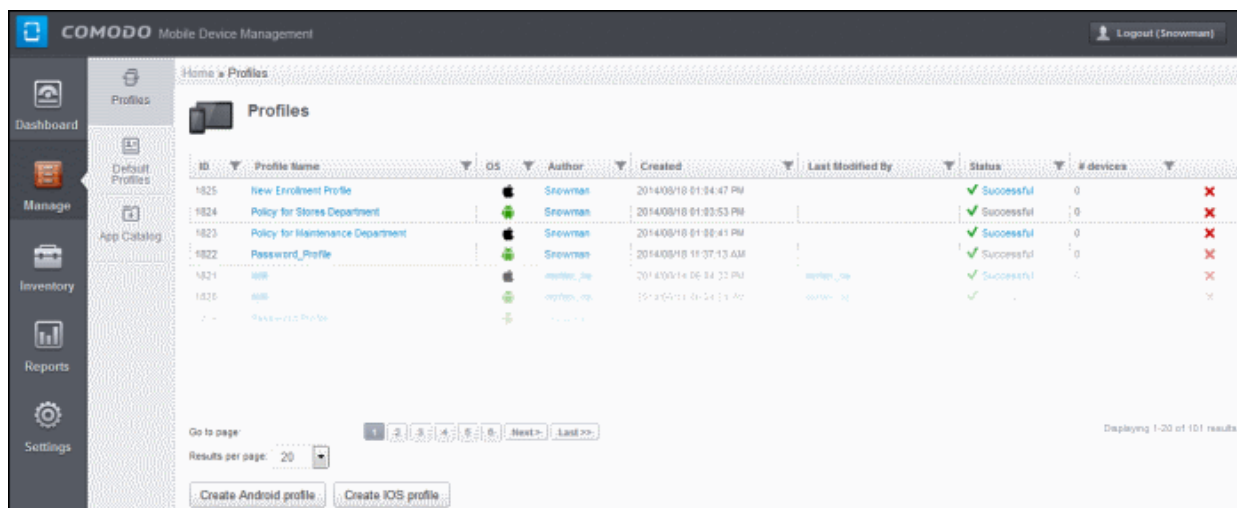
## 4. Managing Configuration Profiles and Apps

A configuration profile is a collection of settings which can be applied to mobile devices that have been enrolled into Comodo Mobile Device Manager. Each profile allows the administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and other general system settings. Profiles are split into iOS profiles and Android profiles. Once created, a profile can be applied to an individual device, to a group of devices or designated as a 'default' profile.

**Profiles** – Contains a list of every iOS and Android profile that has been created. Profiles listed here can be applied to individual devices or designated as a 'default' profile.

**Default Profiles** – Default profiles are those that are automatically applied to a device upon it's initial enrollment into Comodo Mobile Device Manager. Administrators can choose to keep the default profile in place or can subsequently move the device to another profile.

**App Catalog** - The App Catalog interface in CMDM stores the path of Android / iOS apps and used to push them to enrolled devices. It can store apps from Google Play / iOS App Store as well as third party apps. The interface allows to add, delete and update apps in CMDM.

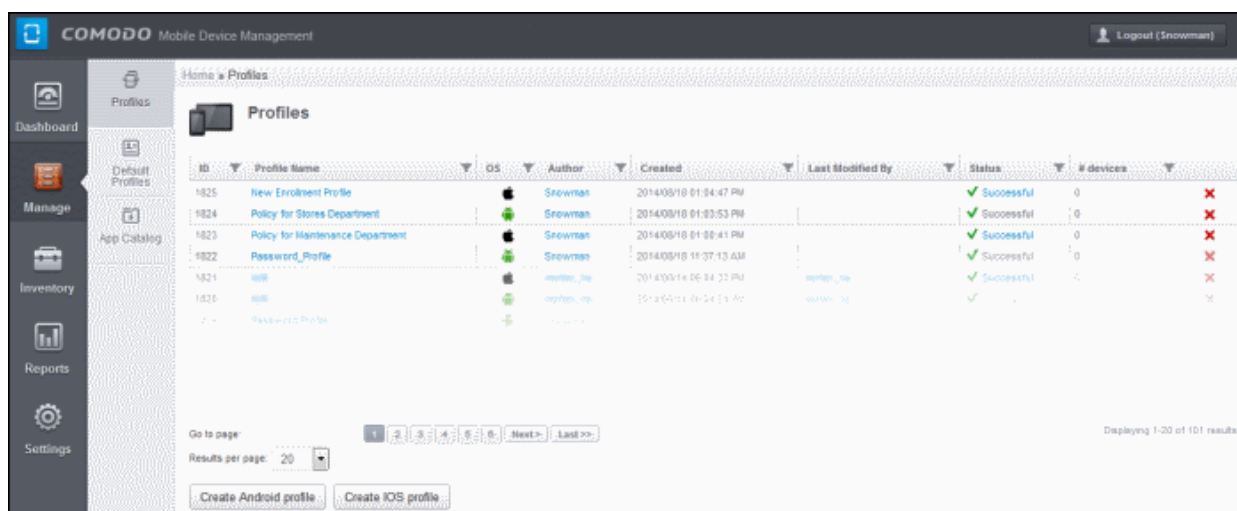


From here an administrator can:

- **Create Configuration Profiles**
- **View the Profiles**
- **Edit Configuration Profiles**
- **Manage Default Profiles**
- **Manage Applications**

## 4.1. Creating Configuration Profiles

The Profiles screen allows you to create new profiles as well as to edit or delete existing profiles in the list. To access this screen, click the Manage tab from the left hand side navigation and then the Profiles tab.



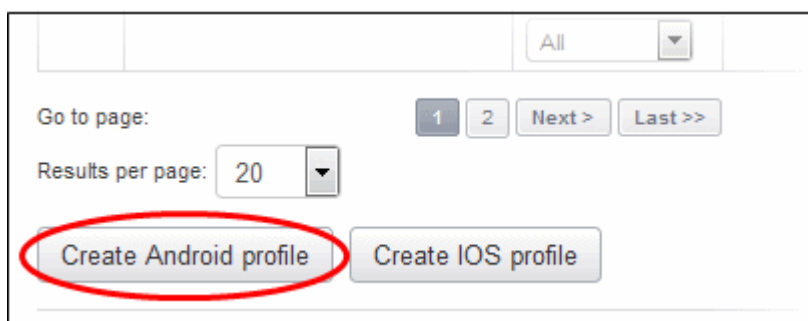
The two buttons at the bottom of the screen allow you to create new profiles for Android and iOS devices. Refer to the next two sections **Profiles for Android Devices** and **Profiles for iOS Devices** for more details.

### 4.1.1. Profiles for Android Devices


To create profiles for Android devices, click the 'Create Android profile' button at the bottom of the Profiles screen.

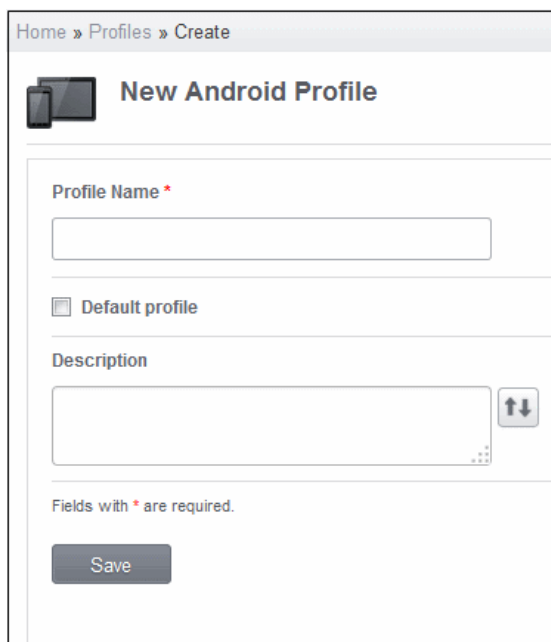
**Note:** Many Android profile settings have blue boxes next to them which indicate the OS and/or device required for the setting to work correctly.

For example, the following box indicates that the setting supports Android 4+ devices and SAFE 1.0+ (Samsung For Enterprises) devices:



The New Android Profile screen will be displayed. Enter the name of the profile and the description for it in the respective fields.

You can also provide a variable in the description field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section [Configuring Custom Variables](#). If you want this profile to be a default policy as well, then select the 'Default profile' checkbox.



- Click the 'Save' button.

Since the General settings such as name and description has been saved, the left side panel will display it as 'Configured' in green. The other items such as Passcode, Restrictions, Antivirus, Wi-Fi settings that are not configured will be displayed as 'Not configured' and will be in gray color.

Home » Profiles » Edit

## Edit Android Profile

**General**  
Configured

**Passcode**  
Not configured

**Restrictions**  
Not configured

**Anti-virus settings**  
Not configured

**Wi-Fi**  
Not configured

**Native App Restrictions**  
Not configured

**Email**  
Not configured

**VPN**  
Not configured

**Kiosk**  
Not configured

**Other Restrictions**  
Not configured

**Network Restrictions**  
Not configured

**Browser Restrictions**  
Not configured

**Bluetooth Restrictions**  
Not configured

**Exchange ActiveSync**  
Not configured

**Profile Name \***

Policy for Stores Department

**Default profile**

**Description**

Profile for stores department

Fields with \* are required.

Save

Click on the following links to know more about each of the settings:

- [Passcode](#)
- [Restrictions](#)
- [Antivirus](#)
- [Wi-Fi](#)
- [Native App Restrictions](#)



- [Email](#)
- [VPN](#)
- [Kiosk](#)
- [Other Restrictions](#)
- [Network Restrictions](#)
- [Browser Restrictions](#)
- [Bluetooth Restrictions](#)
- [Exchange Active Sync](#)

## To configure Passcode settings



- Click anywhere on the Passcode row

The settings screen for Passcode will be displayed.

The screenshot shows the 'Passcode' settings screen. On the left, a sidebar lists various settings categories, all marked as 'Not configured'. The 'Passcode' category is selected and highlighted. The main content area contains the following settings:

- Passcode type:** A dropdown menu currently set to 'No passcode enforcement'.
- Minimum passcode length:** A dropdown menu currently set to '-- Select --'.
- Maximum Idle Time:** A dropdown menu currently set to 'Never timeout'.
- Maximum Failed Attempts:** A dropdown menu currently set to '0'. Below this field, a note states: 'Device will be wiped if this limit exceeds'.
- Maximum passcode age (days):** A text input field with up and down arrow buttons.
- Passcode History Requirements:** A text input field with up and down arrow buttons. A blue badge next to it indicates 'Android 3.0+'. Below this field, a note states: 'Number of previous passcodes from which new passwords must be unique.'.

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

Passcode Configuration – Table of Parameters		
Form Element	Type	Description
Passcode Type	Drop-down	Select the type of passcode from the drop-down that the user should configure for unlocking screen lock. The options available are: <ul style="list-style-type: none"> <li>No passcode enforcement</li> <li>Only letters</li> <li>Letters and numbers</li> <li>Only numbers</li> <li>Letters, numbers and a special symbol</li> <li>Requires some kind of password</li> </ul>
Minimum Passcode Length	Drop-down	Select from the drop-down the minimum passcode length required to be configured by the user. The option is available to set from 4 to 16 characters.
Inactivity Auto-lock	Drop-down	Select the maximum idle time out period to lock the device screen automatically from the drop-down.
Maximum Failed Attempts	Drop-down	Select the maximum number of times the user can attempt unsuccessful logins. The option is available to set from 4 to 16 times and if '0' is selected, the user can attempt any number of times. If the number of failed attempts exceeds the selected number, then the data in the device will be wiped automatically.
Maximum Passcode Age (days)	Text Field	Enter the maximum period in days for which the current passcode could be used. You can also provide a variable in the field by clicking the Insert Variable  button beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Passcode History Requirements	Text Field	This pertains to password reuse policy. This determines the number of unique new passcode that must be associated with the user before an old passcode can be used. You can also provide a variable in the field by clicking the Insert Variable  button beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> . This feature is available for Android 3.0 and later versions only.

- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Passcode section' button at the top.

### To configure Restrictions settings

- Click anywhere on the 'Restrictions' row.

The settings screen for Restrictions will be displayed.

Restrictions Configuration – Table of Parameters		
Form Element	Type	Description
Allow Turn-off WiFi	Checkbox	Select this checkbox if user should be allowed to disable WiFi.
Allow application verification disabling	Checkbox	Select this to allow user to disable 'Verify Apps' option in the security options.
Allow Cellular Data (2g/3g/4g)	Checkbox	Select this if data traffic should be enabled
Allow Turn-off background Sync	Checkbox	Select this to allow users to disable background synchronization setting in their devices.
Allow Bluetooth	Checkbox	Select this if bluetooth should be enabled
Allow Camera	Checkbox	Select this to allow users to use camera
Allow Un-encrypted devices	Checkbox	Select this to enable users to use device without turning on the storage encryption feature. This feature is available for Android 3.0 and later versions only.
Allow Download/Install apps from unknown sources	Checkbox	Select this to allow users to download and install applications from all sources.




- Click the 'Save' button after selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Restrictions section' button at the top.

## To configure Antivirus settings

- Click anywhere on the 'Antivirus settings' row.

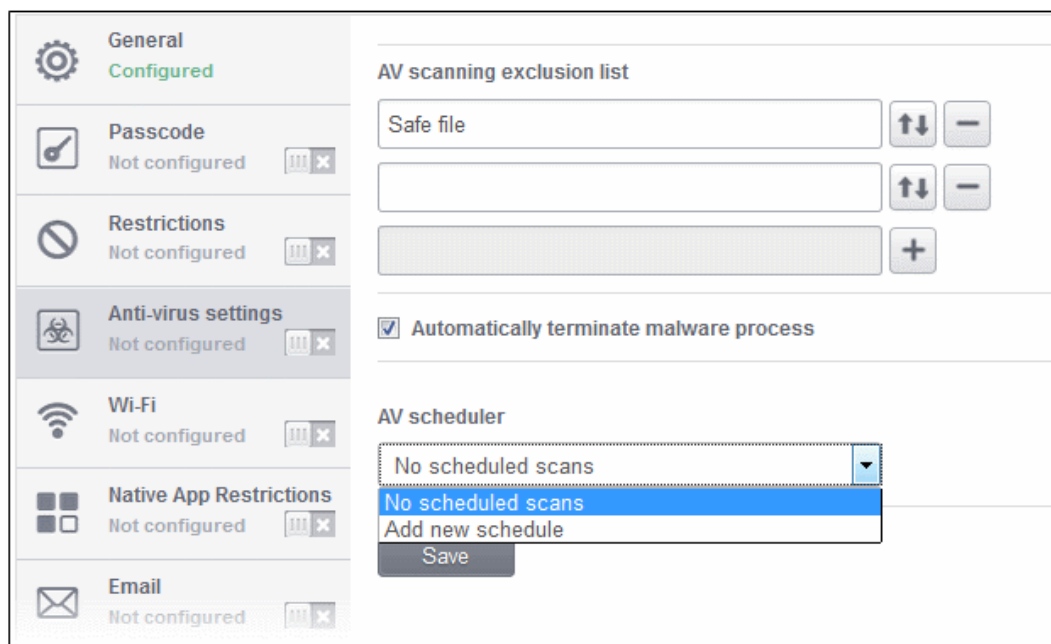
The settings screen for Antivirus will be displayed.

Antivirus Settings – Table of Parameters		
Form Element	Type	Description
AV scanning exclusion list	Text Field	<p>Allows the administrator to add trusted Apps in the field. Antivirus scans will not be performed for these files. Enter the bundle identifier of the app that you want to exclude from antivirus scanning. For example, livio.pack.lang.en_US. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>Click  to add more 'AV scanning exclusions list' fields.</p> <p>To remove an item from the 'AV scanning exclusion list' field, click the  button beside it.</p>

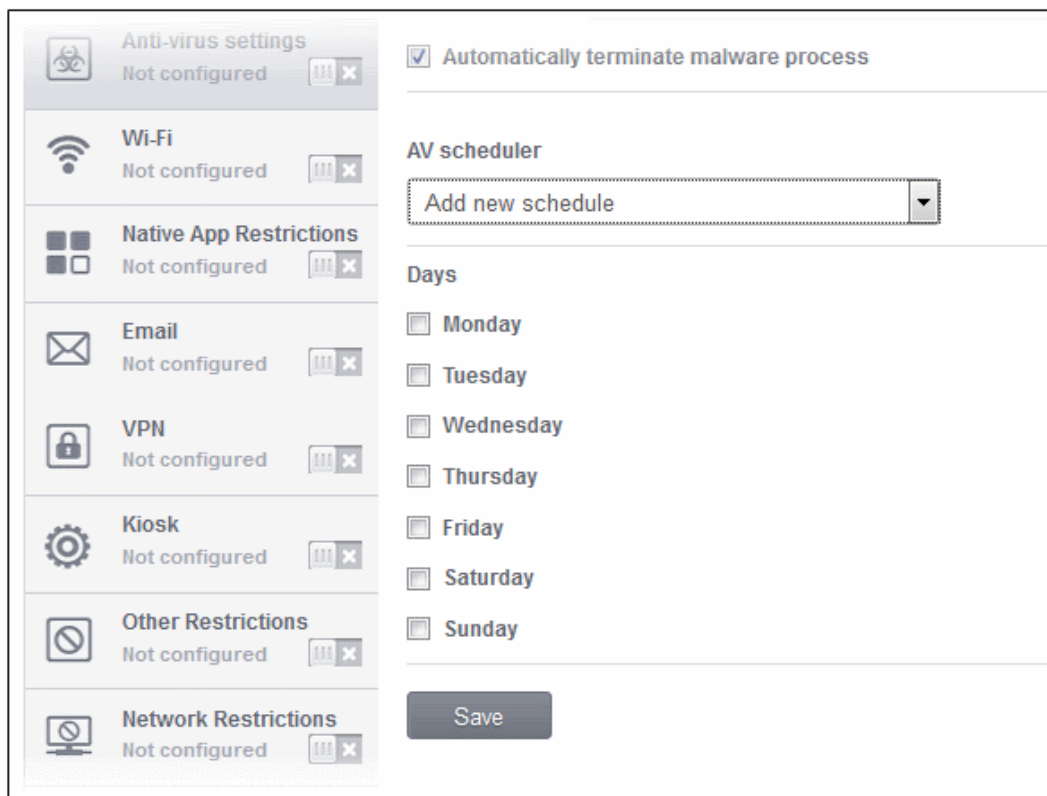
Antivirus Settings – Table of Parameters		
Automatically terminate malware process	Checkbox	If enabled, any malware process detected during scanning will be terminated immediately on the devices. {Patent pending}
No schedule scan	Drop-down	Select if you want to automate the process of antivirus scanning. If you select 'Schedule scan', the option to select the time and day(s) of scheduled scanning will be displayed. Refer to <b>Scheduling Scans</b> for more details.

## Scheduling Scans

If you want to automate the process of antivirus scanning, then select 'Add new schedule' from the drop-down in the 'Antivirus settings' screen.



The option to configure the period will be displayed.



You have the option to select the scan to run daily.

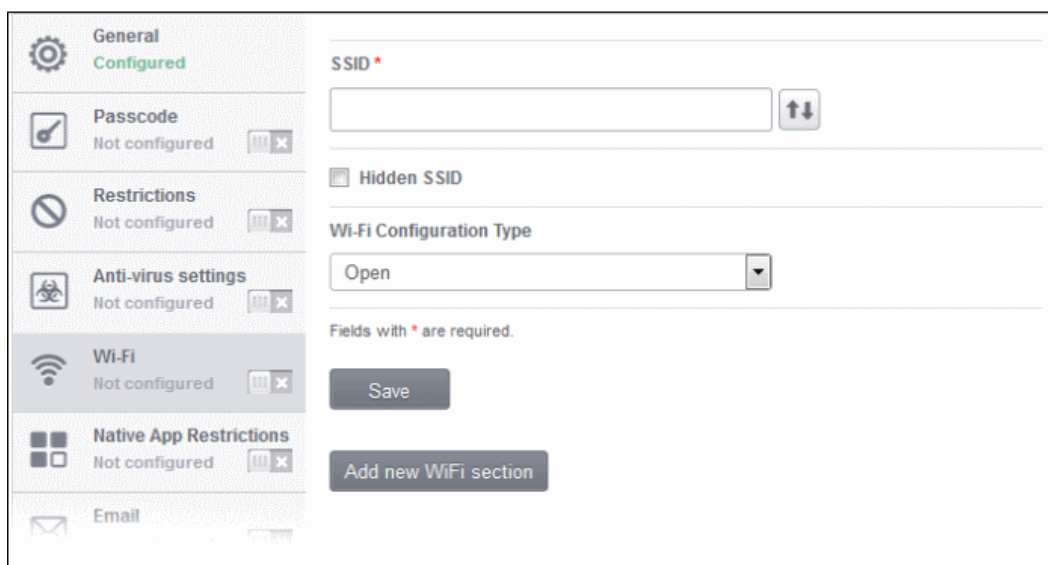
- Select the checkbox beside the day(s) that you want the scheduled scan to run.
- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Antivirus settings section' button at the top.


## To configure Wi-Fi settings

- Click anywhere on the 'Wi-Fi' settings row.



The settings screen for Wi-Fi will be displayed.






Wi-Fi Settings – Table of Parameters		
Form Element	Type	Description
SSID	Text Field	Enter the Service Set Identifier (SSID), the name of the wireless network that a device should connect to. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Hidden SSID	Checkbox	If enabled, users will be able to the access hidden wireless network also. The users must know the hidden SSID details and the required credentials.
Wi-Fi Configuration Type	Drop-down	Select the type of encryption used by the wireless network from the drop-down. The options available are: <ul style="list-style-type: none"> <li>• Open</li> <li>• WEP</li> <li>• WPA / WPA2</li> <li>• 80.1x.EAP</li> </ul> The settings for each type is explained in the next table <b>Wi-Fi configuration type settings</b> .
Add new Wifi section	Button	Click this button to add more wireless networks.

### Wi-Fi Configuration Type settings

Wi-Fi Configuration Type Settings – Table of Parameters	
Security Configuration Type	Description
Open	No password is required for accessing the Wi-Fi network by the user.
WEP	Encryption Key – Enter the password to access the Wi-Fi network. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
WPA / WPA2	Encryption Key – Enter the password to access the Wi-Fi network. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
802.1 x EAP	<p><b>1. EAP Authentication Protocol</b> – Select the EAP authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <ul style="list-style-type: none"> <li>• PEAP</li> <li>• TLS</li> <li>• TTLS</li> </ul> <p><b>2. Phase 2 Authentication Protocol</b> - Select the Phase 2 authentication protocol from the drop-down. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <ul style="list-style-type: none"> <li>• None</li> </ul>

Wi-Fi Configuration Type Settings – Table of Parameters	
	<ul style="list-style-type: none"> <li>• PAP</li> <li>• MSCHAP</li> <li>• MSCHAPV2</li> <li>• GTC</li> </ul> <p><b>3. Certificate</b> – Select the user certificate from the drop-down or upload it using the 'Upload a file' button.</p> <p><b>4. CA Certificate</b> - Select the CA certificate from the drop-down or upload it using the 'Upload a file' button.</p> <p><b>5. Authentication Username</b> – Enter the username for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p><b>6. Authentication Password</b> - Enter the password for Wi-Fi authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p><b>7. Authentication Domain</b> – Enter the details for RADIUS Server authentication. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p><b>8. Anonymous Identity</b> - Enter the username that can be used for anonymous access. Applicable for Samsung for Enterprise devices SAFE 1.0 + version.</p> <p>For items in the list from 5 to 8, you can also provide a variable in the field by clicking the  Insert Variable button beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a>.</p>

- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The newly created profile will now be available in the Profiles List screen and if you have opted for it to be a 'Default profile', it will be available in the 'Default profiles list' as well. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete WiFi section' button at the top.

### To configure native application restrictions

Applications such as Gmail, Email client, Gallery, that come built-in with the device operating system are called native applications. Administrators can choose to allow or deny access to these native applications. The feature is available for Android version 4.0 + and Samsung for Enterprise devices SAFE 1.0 + version.

**Note:** Email client would not be able to be restricted if an Exchange Mail is already configured with device admin rights. Refer to the section [Exchange Active Sync](#) for more details.

- Click anywhere on the 'Native Application Restrictions' settings row.

The settings screen for Native App Restrictions will be displayed.

Setting	Version Requirement
<input checked="" type="checkbox"/> Allow Gmail	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Email	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Browser	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Gallery	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Settings	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Google Play	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Youtube App	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Google Maps & Navigation	Android 4.0+/SAFE 1.0+
<input checked="" type="checkbox"/> Allow Google and Voice Search	Android 4.0+/SAFE 1.0+

**Native Application Restrictions Settings – Table of Parameters**

Form Element	Type	Description
Allow Gmail	Checkbox	Select this to allow users to access Gmail app.
Allow Email	Checkbox	Select this to allow users to access default Email app.
Allow Browser	Checkbox	If enabled, users can access default browser on their devices.
Allow Gallery	Checkbox	If enabled, users can access Gallery on their devices.
Allow Settings	Checkbox	Select this to enable users to change device settings.
Allow Google Play	Checkbox	If enabled, users can access Google Play on their mobile devices.
Allow YouTube App	Checkbox	If enabled, users can access YouTube.
Allow Google Maps & Navigation	Checkbox	If enabled, users can access Google Maps and Navigation app on their via mobile devices.
Allow Google and Voice Search	Drop-down	If enabled, users can use Google and Voice Search services.

- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Native App Compliance section' button at the top.







### To configure email settings



The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click anywhere on the 'Email' settings row.

The settings screen for Email will be displayed.

<b>General</b> Configured	Configure for Type * <span style="float: right;">SAFE 2.0+</span> IMAP
<b>Passcode</b> Not configured	Email address * <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Restrictions</b> Not configured	Account Display Name <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Anti-virus settings</b> Not configured	<input checked="" type="checkbox"/> Set as Default Account <span style="float: right;">SAFE 2.0+</span>
<b>Wi-Fi</b> Not configured	Mail Server Host Name (for Incoming Mail) * <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Native App Restrictions</b> Not configured	Mail Server Port Number (for Incoming Mail) * <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Email</b> Not configured	<input checked="" type="checkbox"/> Use SSL (for Incoming Mail) <span style="float: right;">SAFE 2.0+</span>
<b>VPN</b> Not configured	<input checked="" type="checkbox"/> Accept All Certificates (for Incoming Mail) <span style="float: right;">SAFE 2.1+</span>
<b>Kiosk</b> Not configured	<input checked="" type="checkbox"/> Accept TLS Certificates (for Incoming Mail) <span style="float: right;">SAFE 2.0+</span>
<b>Other Restrictions</b> Not configured	Mail Server Host Name (for Outgoing Mail) * <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Network Restrictions</b> Not configured	Mail Server Port Number (for Outgoing Mail) * <span style="float: right;">SAFE 2.0+</span> <input type="text"/>
<b>Browser Restrictions</b> Not configured	<input checked="" type="checkbox"/> Use SSL (for Outgoing Mail) <span style="float: right;">SAFE 2.0+</span>
<b>Bluetooth Restrictions</b> Not configured	<input checked="" type="checkbox"/> Accept All Certificates (for Outgoing Mail) <span style="float: right;">SAFE 2.1+</span>
<b>Exchange ActiveSync</b> Not configured	<input checked="" type="checkbox"/> Accept TLS Certificates (for Outgoing Mail) <span style="float: right;">SAFE 2.0+</span>
	Sender Name <span style="float: right;">SAFE 3.0+</span> <input type="text"/>
	Set Signature <span style="float: right;">SAFE 3.0+</span> <input type="text"/>
	<input checked="" type="checkbox"/> Prevent Moving Mail to other Accounts <span style="float: right;">SAFE 3.0+</span>
	<input type="checkbox"/> Always Vibrate on New Email Notification <span style="float: right;">SAFE 3.0+</span>
	<input type="checkbox"/> Vibrate on New Email Notification if device is silent <span style="float: right;">SAFE 3.0+</span>
	<input type="button" value="Save"/>

Email Settings – Table of Parameters		
Form Element	Type	Description
Configure for Type*	Drop-down	Select IMAP or POP for which you want to configure the settings.
Email address*	Text Field	Click the Insert Variable button  beside the field, select '%u.mail%' from the 'Variables list' and click 'Apply'. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Account Display Name	Text Field	Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Set as Default Account	Checkbox	If enabled, the email account will be set as default for the users.
Mail Server Host Name (for Incoming Mail) *	Text Field	Enter the host name of the incoming mail server or its IP address. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Mail Server Port Number (for Incoming Mail) *	Text Field	Enter the server port number used for incoming mail service. For POP3, it is usually 110 and if SSL is enabled it is 995. For IMAP, it is usually 143 and if SSL is enabled it is 993. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Use SSL (for Incoming Mail)	Checkbox	If enabled, communication between incoming mail server and devices is encrypted using SSL (Secure Socket Layer Protocol).
Accept All Certificates (for Incoming Mail)	Checkbox	If enabled, automatically accepts all SSL certificates.
Accept TLS Certificates (for Incoming Mail)	Checkbox	If enabled, automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol).
Mail Server Host Name (for Outgoing Mail) *	Text box	Enter the host name or IP address for the outgoing mail server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Mail Server Port Number (for Outgoing Mail) *	Text box	Enter the server port number used for outgoing mail service. If no port number is specified then ports 25, 587 and 465 are used in the given order. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Use SSL (for Outgoing Mail)	Checkbox	If enabled, communication between outgoing mail server and devices is encrypted using SSL.
Accept All Certificates (for Outgoing Mail)	Checkbox	If enabled, automatically accepts all SSL certificates.

Email Settings – Table of Parameters		
Accept TLS Certificates (for Outgoing Mail)	Checkbox	If enabled, automatically accepts all secure certificates for TLS (Transport Secure Layer Protocol).
Sender Name	Text Field	Enter the name of the user that will appear as Sender in the sent messages. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Set Signature	Text Field	Enter the signature and other details that will appear at the end of the sent messages. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Prevent Moving Mail to other Accounts	Checkbox	If enabled, the user cannot move sent or received mails to another account.
Always Vibrate on New Email Notification	Checkbox	If enabled, the device will vibrate in addition to sound alert when a new email is received.
Vibrate on New Email Notification if device is silent	Checkbox	If enabled, the device will vibrate when a new email is received.

Fields with \* are mandatory.

- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Email section' button at the top.



### To configure VPN settings




The feature is supported for Samsung for Enterprise (SAFE) devices only

- Click anywhere on the 'VPN' row.

The settings screen for VPN will be displayed.



VPN Settings – Table of Parameters		
Form Element	Type	Description
Connection for type	Drop-down	Select the VPN connection type from drop-down. The options available are: L2TP, PPTP, L2TP/IPSec PSK and IPSec XAuth PSK.
VPN Connection Name	Text Field	Enter the name of the connection, which will be displayed on the device. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Host name of the VPN Server	Text Field	Enter the host name of the VPN server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .

VPN Settings – Table of Parameters		
Username	Text Field	Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Password	Text Field	Leave the field blank. The user will be prompted to enter to the password while trying to connect to VPN.
DNS Search Domains	Text Field	Enter the IP address of the DNS server that devices will use for searching domain names. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
If L2TP is selected:		
<ul style="list-style-type: none"> <li>• Enable L2TP Secret</li> </ul>	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
<ul style="list-style-type: none"> <li>• L2TP Secret</li> </ul>	Text Field	If L2TP Secret is enabled, then the pre-shared key should be entered here by the user.
If PPTP is selected:		
<ul style="list-style-type: none"> <li>• Enable Encryption</li> </ul>	Checkbox	If selected, the connection is encrypted between the devices and the VPN server.
If L2TP/IPSec PSK is selected:		
<ul style="list-style-type: none"> <li>• IPSec Pre-Shared Key</li> </ul>	Text Field	If IP Sec Identifier is enabled, then the pre-shared key should be entered here by the user.
<ul style="list-style-type: none"> <li>• Enable L2TP Secret</li> </ul>	Checkbox	If enabled, the pre-shared L2TP should be entered in the next field L2TP Secret
<ul style="list-style-type: none"> <li>• L2TP Secret</li> </ul>	Text Field	If L2TP Secret is enabled, then the pre-shared key should be entered here by the user.
If IPSec Xauth PSK is selected:		
<ul style="list-style-type: none"> <li>• IP Sec Identifier</li> </ul>	Text Field	Enter the IPSec identifier in the field. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
<ul style="list-style-type: none"> <li>• IPSec Pre-Shared Key</li> </ul>	Text Field	If IP Sec Identifier is enabled, then the pre-shared key should be entered here by the user.

- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete VPN section' button at the top.

## To configure Kiosk settings








Supported for Samsung for Enterprise (SAFE) devices only.

Kiosk mode is a feature intended to help administrators lock-down mobile devices by limiting the applications that are able to run on a device. The main goal of Kiosk mode is to lock a device into a particular application, to either allow a single app or multiple apps, to take over the screen of a device, such as in-house applications, or to prevent users from opening other applications that

should not be accessible to them, such as in retail environments. For example, if employees are using an Galaxy Tab for a corporate app, or admins simply need to ensure devices are only running a single application - Kiosk mode will ensure your devices are being used as intended.

To access kiosk settings, click anywhere on the 'Kiosk' row. The Kiosk settings screen will be displayed:

Kiosk Settings – Table of Parameters		
Form Element	Type	Description
Kiosk Mode Type	Drop-down	<p>The two Kiosk modes are:</p> <ul style="list-style-type: none"> <li>Default mode - Run multiple apps in Kiosk mode. Users will not be able to run non-kiosk applications. Kiosk mode can only be exited by entering the admin bypass password.</li> <li>Single App mode – Users can only run the single application that you specify. Users will not be able to run non-kiosk applications. Kiosk mode can only be exited if the admin disables it in the CMDM console.</li> </ul> <p>Restrictions on access to other device functions, such as task manager and the status bar, can also be configured for either mode.</p>
Block Multi-Window Mode	Checkbox	If selected, users cannot open multiple windows.
Block Task Manager	Checkbox	If selected, users cannot access task manager screen.
Hide Navigation Bar	Checkbox	If selected, the navigation bar will be hidden on the devices.

Kiosk Settings – Table of Parameters		
Hide Status Bar	Checkbox	If selected, the status bar will not be displayed.
Hide System Bar	Checkbox	If selected, the system bar will not be displayed.
Block Hardware Keys	Text Field	<p>This feature allows to block keypad buttons available on the devices. For example, if you do not want the device owners to use Caps Lock key and so on, then these can be blocked.</p> <p>Click the Insert Variable button  beside the field, select the key that you want to block from the list and click OK. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>Click  to add more 'Block Hardware Keys' fields.</p> <p>To remove a field, click the  button beside it.</p>
If 'Single App' is selected as Kiosk Mode Type:		
App ID for allowed Apps in Kiosk Mode	Text Field	Enter the ID of the app that will run in Kiosk mode.
If 'Default mode' is selected as Kiosk Mode Type:		
App ID for allowed Apps in Kiosk Mode	Text Field	<p>Enter the ID of the apps that will run in Kiosk mode. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>Click  to add more 'App IDs for allowed Apps om Kiosk Mode' fields.</p> <p>To remove a field, click the  button beside it.</p>
Show messenger App	Checkbox	If selected, the messenger app will be available.
Show email App	Checkbox	If selected, email app will be available.
Show dialer App	Checkbox	If selected, dialer app will be available.
Show admin bypass button	Checkbox	If selected, the 'Admin bypass button' will be available, which an admin can tap, enter the password to exit from the Kiosk mode.
Admin bypass password	Text Field	<p>Enter the password required to exit the Kiosk mode. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p>

- Click the 'Save' button after entering or selecting the parameters.

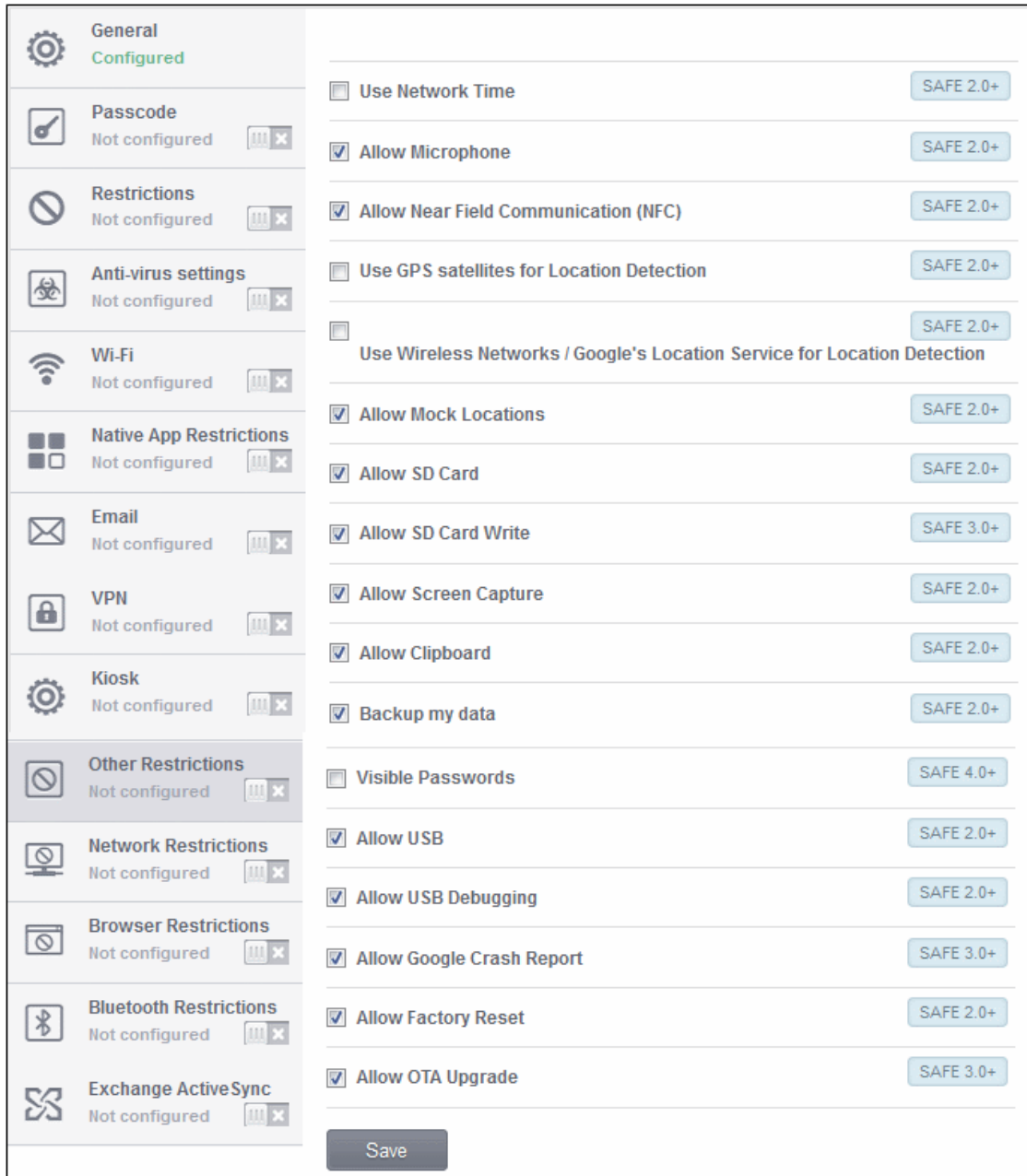
A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Kiosk section' button at the top.

## To configure Other Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click anywhere on the 'Other Restrictions' row.

The settings screen for Other Restrictions will be displayed.



Other Restrictions Settings – Table of Parameters		
Form Element	Type	Description
Use Network Time	Checkbox	Allows users to enable/disable network provided values in Date & Time settings.
Allow Microphone	Checkbox	Allows users to use microphone. If this is disabled, users can use microphone for receiving and making calls only.
Allow Near Field Communication (NFC)	Checkbox	Allows devices to establish connection via NFC
Use GPS satellites for Location Detection	Checkbox	Allows users to enable/disable GPS system for location detection.
Use Wireless Networks / Google's Location Service for Location Detection	Checkbox	Allows users to enable /disable Wireless Networks / Google's Location Service for location detection
Allow Mock Locations	Checkbox	Allows users to enable/disable 'Mock Location' in developer mode settings.
Allow SD Card	Checkbox	Users can use SD card on their devices.
Allow SD Card Write	Checkbox	Users can store data on the SD card.
Allow Screen Capture	Checkbox	Users can take screenshot of the device screen.
Allow Clipboard	Checkbox	Users will be allowed to use clipboard memory.
Backup my data	Checkbox	Users will be allowed to take a backup of data in their devices.
Visible Passwords	Checkbox	Allows users to enable/disable show password feature.
Allow USB	Checkbox	Allows users to establish connections via USB ports.
Allow USB Debugging	Checkbox	Allows users to enable/disable 'USB Debugging' option in developer mode settings.
Allow Google Crash Report	Checkbox	Crash reports will be sent to Google.
Allow Factory Reset	Checkbox	Users are allowed to reset the device to factory settings.
Allow OTA Upgrade	Checkbox	Over-the-air (OTA) upgrade is the wireless delivery of data or new software to mobile phones and tablets.

- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Other restrictions section' button at the top.

### To configure Network Restrictions settings



The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click anywhere on the 'Network Restrictions' row.

The settings screen for Network Restrictions will be displayed.







The screenshot shows the 'Network Restrictions' settings page. The sidebar on the left includes: General (Configured), Passcode (Not configured), Restrictions (Not configured), Anti-virus settings (Not configured), Wi-Fi (Not configured), Native App Restrictions (Not configured), Email (Not configured), VPN (Not configured), Kiosk (Not configured), Other Restrictions (Not configured), **Network Restrictions (Not configured)**, Browser Restrictions (Not configured), Bluetooth Restrictions (Not configured), and Exchange ActiveSync (Not configured). The main content area includes:
 

- Wi-Fi Network Minimum Security Level: Open (SAFE 2.0+)
- Allow user to add Wi-Fi networks:  (SAFE 2.0+)
- Allow wi-fi access point settings editing:  (SAFE 2.2+)
- Allow USB Tethering:  (SAFE 2.2+)
- Allow Data Roaming:  (SAFE 2.2+)
- Allow Sync during Roaming:  (SAFE 1.0+)
- Allow Voice Roaming:  (SAFE 3.0+)
- Allow Emergency Calls only:  (SAFE 2.0+)
- Allow SMS: All (SAFE 3.0+)
- Allow MMS: All (SAFE 3.0+)
- Whitelisted SSIDs: (SAFE 2.2+)
- Blacklisted SSIDs: (SAFE 2.2+)

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

**Network Restrictions Settings – Table of Parameters**

Form Element	Type	Description
Wi-Fi Network Minimum Security Level	Drop-down	Select the minimum security level required for the user to access the Wi-Fi network. The options available are: <ul style="list-style-type: none"> <li>• Open</li> <li>• WEP</li> <li>• WPA</li> <li>• 802.1x EAP (LEAP)</li> </ul>

Network Restrictions Settings – Table of Parameters		
		<ul style="list-style-type: none"> <li>802.1x EAP (FAST)</li> <li>802.1x EAP (PEAP)</li> <li>802.1x EAP (TTLS)</li> <li>802.1x EAP (TLS)</li> </ul>
Allow user to add Wi-Fi networks	Checkbox	Allows users to add Wi-Fi networks in their devices.
Allow Wi-Fi access point settings editing	Checkbox	Allows users to edit the Wi-Fi access point settings.
Allow USB Tethering	Checkbox	Allows users to share USB with other similar devices.
Allow Data Roaming	Checkbox	Allows users to enable/disable data roaming option in their devices.
Allow Sync during Roaming	Checkbox	Allows the use of Sync feature while roaming.
Allow Voice Roaming	Checkbox	Allows users to make/receive voice call during roaming.
Allow Emergency Calls only	Checkbox	Allows users to make emergency calls only.
Allow SMS	Drop-down	Allows text messages per the options selected: <ul style="list-style-type: none"> <li>All – Allows both incoming and outgoing text messages.</li> <li>Incoming SMS only – Allows incoming text messages only.</li> <li>Outgoing SMS only – Allows outgoing text messages only.</li> <li>None – Both incoming and outgoing text messages are blocked.</li> </ul>
Allow MMS	Drop-down	Allows multimedia messages per the options selected: <ul style="list-style-type: none"> <li>All – Allows both incoming and outgoing multimedia messages.</li> <li>Incoming SMS only – Allows incoming multimedia messages only.</li> <li>Outgoing SMS only – Allows outgoing multimedia messages only.</li> <li>None – Both incoming and outgoing multimedia messages are blocked.</li> </ul>
Whitelisted SSIDs	Text Field	Specify the name (SSID) of the wireless network that should be whitelisted. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> . Click the  button to add more 'Whitelisted SSID' fields. To remove a Whitelisted SSID field from the screen, click the minus  button beside it.
Blacklisted SSIDs	Text Field	Specify the name (SSID) of the wireless network that should be blacklisted. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> . Click the  button to add more 'Blacklisted SSID' fields. To remove a Blacklisted SSID field from the screen, click the minus  button beside it.

- Click the 'Save' button.

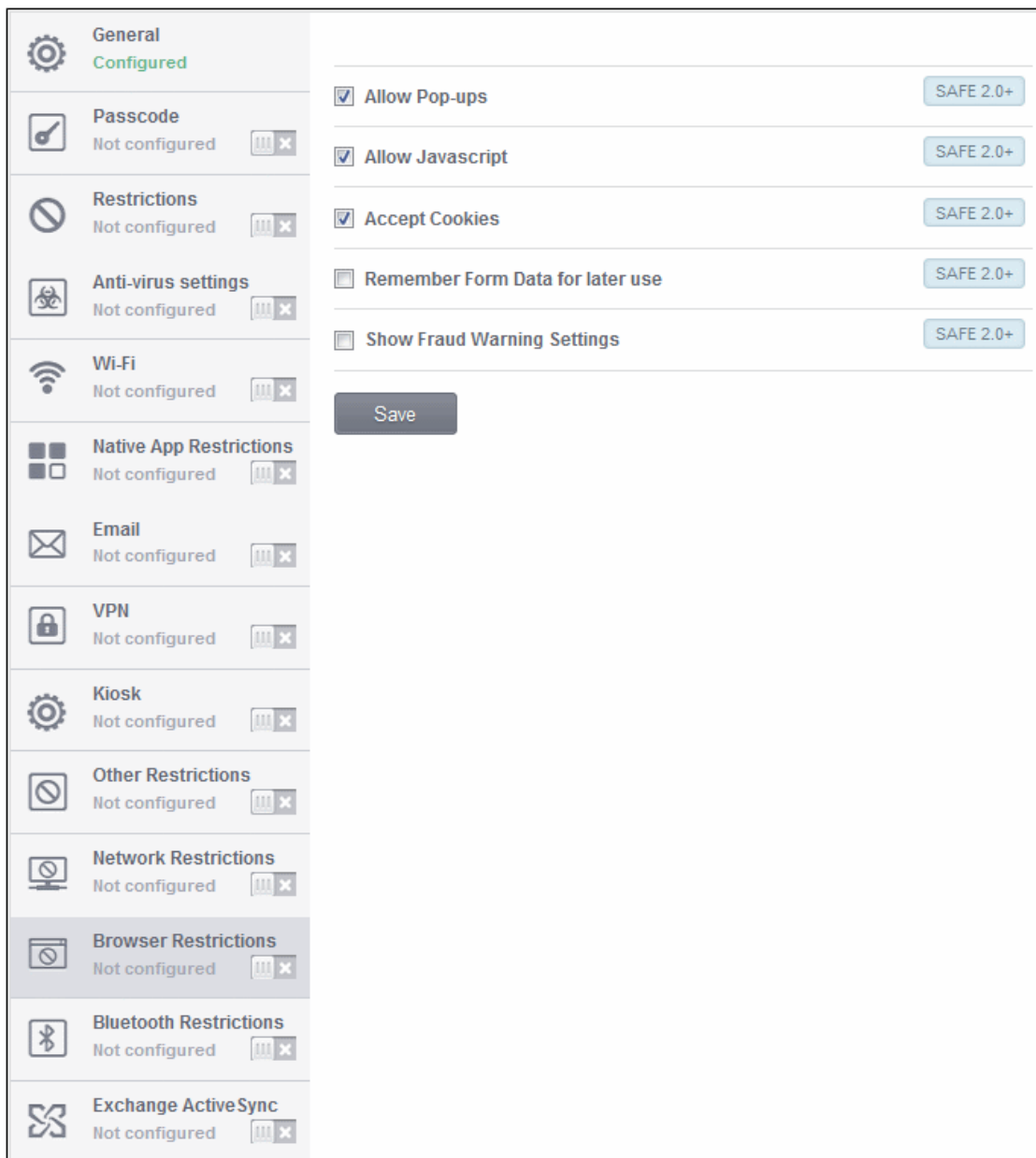
A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Network Restrictions section' button at the top.

### To configure Browser Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click anywhere on the 'Browser Restrictions' row.

The settings screen for Browser Restriction will be displayed.



Browser Restrictions Settings – Table of Parameters		
Form Element	Type	Description
Allow Pop-ups	Checkbox	Pop-ups in browsers will be allowed in the users' devices.
Allow Javascript	Checkbox	Applications running on Java scrips will be allowed.

Browser Restrictions Settings – Table of Parameters		
Accept Cookies	Checkbox	Users will be allowed to modify Cookies settings on their devices.
Remember Form Data for later use	Checkbox	Users will be allowed to use Auto Fill settings on their devices.
Show Fraud Warning Settings	Checkbox	Users will be allowed to use Fraud Warning Settings on their devices.

- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Browser Restrictions section' button at the top.

#### To configure Bluetooth Restrictions settings

The feature is supported for Samsung for Enterprise (SAFE) devices only.

- Click anywhere on the 'Bluetooth Restrictions' row.

The settings screen for Bluetooth Restrictions will be displayed.

Bluetooth Restrictions Settings – Table of Parameters		
Form Element	Type	Description
Allow Device discovery via Bluetooth	Checkbox	Allows discovery of other devices via Bluetooth.
Allow Bluetooth Pairing	Checkbox	Allows users' devices to pair with other their devices via Bluetooth.
Allow Outgoing Calls	Checkbox	Allows users to make calls using Bluetooth enabled devices (eg. hands-free devices)
Allow Bluetooth Tethering	Checkbox	Allows users to enable/disable Bluetooth tethering option.
Allow connection to Desktop or Laptop via Bluetooth	Checkbox	Allow users to enable/disable Bluetooth connection with Desktop or Laptop.
Allow data transfer	Checkbox	Allows data transfer between devices via Bluetooth.

- Click the 'Save' button.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Bluetooth Restrictions section' button at the top.

## To configure Exchange ActiveSync settings

CMDM allows you to configure users to access their mail accounts in Exchange Server. Refer to the section Installing Exchange Service for more details.

**Note:** Please make sure that the intended users are not restricted to use Email client on their devices. Refer to the section **Native App Restriction** for more details.

- Click anywhere on the 'Exchange ActiveSync' row.

The settings screen for Exchange ActiveSync will be displayed.

- General**  
Configured
- Passcode**  
Not configured
- Restrictions**  
Not configured
- Anti-virus settings**  
Not configured
- Wi-Fi**  
Not configured
- Native App Restrictions**  
Not configured
- Email**  
Not configured
- VPN**  
Not configured
- Kiosk**  
Not configured
- Other Restrictions**  
Not configured
- Network Restrictions**  
Not configured
- Browser Restrictions**  
Not configured
- Bluetooth Restrictions**  
Not configured
- Exchange Active Sync**  
Not configured

**Email Address \*** SAFE 2.0+

 ↑↓


---

**User Name \*** SAFE 2.0+

 ↑↓


---

**Domain \*** SAFE 2.0+

 ↑↓


---

**Server Address \*** SAFE 2.0+

 ↑↓


---

**Password** SAFE 2.0+





 ↑↓


---

Fields with \* are required.

Save



Exchange ActiveSync Configuration – Table of Parameters		
Form Element	Type	Description
Email Address *	Text Field	Click the 'Insert Variable' button  beside the field, select '%u.mail' from the User Variables' list and click 'Apply'. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
User Name *	Text Field	Click the 'Insert Variable' button  beside the field, select '%u.login' from the User Variables' list and click 'Apply'. The username of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Domain *	Text Field	Enter the domain name in the field. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Server Address *	Text Field	Enter the server address of the ActiveSync. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Password *	Text Field	Leave the field blank. The user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.

Fields with \*are mandatory.

- Click the 'Save' button.

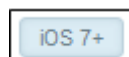
A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Antivirus settings section' button at the top.

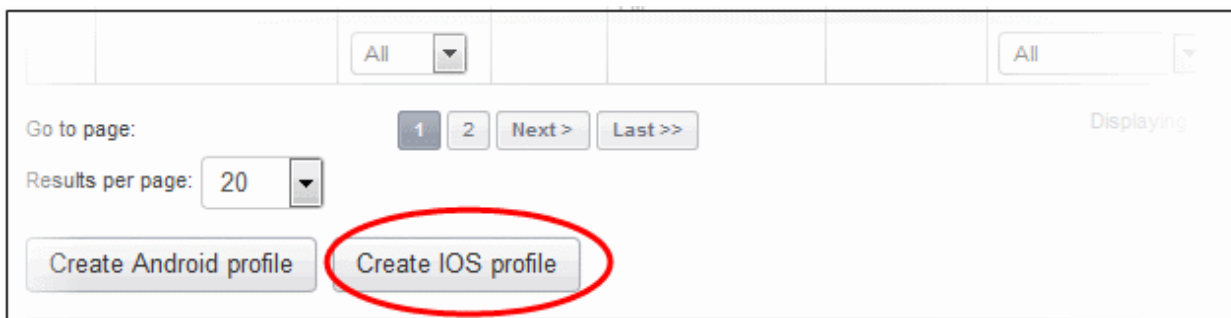
## 4.1.2. Profiles for iOS Devices

To create profiles for iOS, click the 'Create iOS profile' link at the bottom of the Profiles screen.

**Note:** Many iOS profile settings have blue boxes next to them which indicate the iOS version required for the setting to work correctly.

For example, the following box indicates that the setting supports Apple devices with iOS version 7 and above only:







The General Settings of the New iOS Profile screen will be displayed.

The screenshot shows the 'New iOS Profile' configuration screen. The breadcrumb trail is 'Home » Profiles » Create'. The title is 'New iOS Profile' with a mobile device icon. The form contains the following elements:

- Profile Name \***: A text input field with the placeholder text 'Display name of the profile (shown on the device)'.
- Default profile**: A checkbox.
- Description**: A text area with a placeholder text 'Brief explanation of the contents or purpose of the profile' and an 'Insert Variable' button (up and down arrows).
- Consent text**: A text area with a placeholder text 'Brief message that will be displayed during profile installation' and an 'Insert Variable' button (up and down arrows).
- Fields with \* are required.**
- Save**: A button at the bottom left.

General Settings – Table of Parameters		
Form Element	Type	Description
Profile Name	Text Field	Enter the name of the profile. This need not be unique but better to provide a descriptive name that matches the profile.
Default profile	Checkbox	Select this checkbox if the profile should be also a default profile.
Description	Text Field	Enter the description for the profile. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section

General Settings – Table of Parameters		
		<b>Configuring Custom Variables.</b>
Consent Text	Text Field	Enter a consent message in the field that will be displayed in the user's device when the profile is being installed. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b>

- Click the 'Save' button after selecting the parameters.

Since the General settings has been saved, the left side panel will display it as 'Configured' in green. The other items in the panel will be in gray color.

Click on the following links to know more about each of the settings:

- [Passcode](#)
- [AirPlay](#)
- [AirPrint](#)
- [Restrictions](#)
- [Wi-Fi](#)
- [VPN](#)
- [Per-App VPN](#)
- [Mail](#)
- [Exchange Active Sync](#)
- [LDAP](#)
- [Calendar](#)
- [Subscribed Calendars](#)
- [Contacts](#)
- [Global HTTP Proxy](#)
- [Web Clip](#)
- [APN](#)
- [Cellular Networks](#)
- [Single Sign-On](#)

## To configure Passcode settings

- Click anywhere on the Passcode row.

The settings screen for Passcode will be displayed.

- General**  
Configured
- Passcode**  
Not configured
- AirPlay**  
Not configured
- AirPrint**  
Not configured
- Restrictions**  
Not configured
- Wi-Fi**  
Not configured
- VPN**  
Not configured
- Per-App VPN**  
Not configured
- Mail**  
Not configured
- Exchange ActiveSync**  
Not configured
- LDAP**  
Not configured
- Calendar**  
Not configured
- Subscribed Calendars**  
Not configured
- Contacts**  
Not configured
- Global HTTP proxy**  
Not configured
- Web Clip**  
Not configured

**Allow simple value**  
Permit the use of repeating, ascending, and descending character sequences

**Require alphanumeric value**  
Require passcodes to contain at least one letter

**Minimum passcode length**  
  
Minimum number of passcode characters allowed

**Minimum number of complex characters**  
  
Minimum number of non-alphanumeric characters allowed

**Maximum passcode age**  
  
Days (1-730) after which passcode must be changed



**Maximum Idle Time**  
  
Device automatically locks when minutes elapse

**Passcode history**  
  
The number (1-50) of unique passcodes required before reuse

**Maximum grace period for device lock**  
  
Maximum amount of time device can be locked without prompting for passcode on unlock

**Maximum number of failed attempts**  
  
Number of passcode entry attempts allowed before all data on device will be erased

Fields with \* are required.

Passcode Configuration – Table of Parameters		
Form Element	Type	Description
Allow Simple Value	Checkbox	Selecting this will allow the users to configure repeated or sequential characters in their passwords. For example, '9999' or ABCD.
Require Alphanumeric Value	Checkbox	Selecting this will compel the user to configure at least one number or letter in their passwords.
Minimum Passcode Length	Drop-down	The minimum number of characters that a password should contain. The option is available to set from 1 to 16.
Minimum Number of Complex Characters	Drop-down	The minimum number of symbols (non alphanumeric characters such as *, %, @) that a password should contain. The option is available to set from 1 to 4.
Maximum Passcode Age	Text Field	Enter the maximum number of days that a password can be valid. The option is available from 1 day to 730 days. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Maximum Idle Time	Drop-down	Select the period of time in minutes that a device can be idle before it's screen is automatically locked.
Passcode History	Text Field	New passwords should not match previously used passwords. Specify the number of last used passwords that should be stored for comparison. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Maximum Grace Period for Device Lock	Drop-down	Select the period from the drop-down how soon the device can be unlocked since last used without prompting the user to enter the password. The option is available from 'Immediately' to '4 Hours' If 'Immediately' is selected, the user has to enter the password each time the device is unlocked.
Maximum Number of Failed Attempts	Drop-down	Select the number of unsuccessful login attempts that can be tried by a user before the device is wiped clean of all its data and settings. The option is available to set from 4 to 10. After 6 unsuccessful login attempts, there will be a time delay before a password can be entered again and the time delay period increases with each failed login attempt. This time delay begins only after the sixth attempt, so if you select the period as 6 or lower, there will be no time delay and data will be erased after the final attempt.






- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Passcode section' button at the top.


## To configure AirPlay settings

**Note:** This settings is applicable for devices that runs on iOS 7 and later versions.

The settings screen for AirPlay will be displayed.

AirPlay Settings Configuration – Table of Parameters		
Form Element	Type	Description
Device ID	Text Field	<p>Enter the device ID of AirPlay destinations that you want to whitelist. The ID numbers of the devices should be entered in the format as given below: XX:XX:XX:XX:XX:XX</p> <p>You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>Click  button to add more 'Device ID' fields. To remove a AirPlay destination device from the screen, click the  button beside it.</p> <p>Note: This setting is applicable for supervised devices only.</p>
Device name	Text Field	<p>Enter the name of the AirPlay destination device that you entered above. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>Click  button to add more 'Device name' and 'Password' fields. To remove a AirPlay device from the screen, click the x button beside it.</p>



AirPlay Settings Configuration – Table of Parameters		
Password	Text Field	Enter the password for the AirPlay destination that you entered above. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Add new AirPlay section	Button	Click this button to add another AirPlay section.



- Click the 'Save' button after entering or selecting the parameters.


A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete AirPlay section' button at the top.

## To configure AirPrint settings

**Note:** This settings is applicable for devices that runs on iOS 7 and later versions.

The settings screen for AirPrint will be displayed.

AirPrint Settings Configuration – Table of Parameters		
Form Element	Type	Description
IP Address	Text Field	Enter the device ID of AirPrint destination (printer). You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .  Click the  button to add more 'IP address' and 'Resource path' fields. To remove an AirPrint device from the screen, click the x button beside it.
Resource Path	Text Field	Enter the resource path of the printer, for example,

AirPrint Settings Configuration – Table of Parameters		
		printers/ HP_LaserJetPro_M1136_series. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Add new AirPrint section	Button	Click this button to add another AirPrint section.

- Click the 'Save' button after entering or selecting the parameters.


A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete AirPrint section' button at the top.

### To configure Restrictions settings

- Click anywhere on the 'Restrictions' row.

The settings screen for Restrictions will be displayed. It is divided into five main sections:

- **Device functionality**
- **Applications**
- **iCloud**
- **Security and privacy**
- **Content ratings**

You can expand/collapse a section by clicking the  button beside each section head.

## Device Functionality

▲

### Device functionality

Enable use of device features

<input checked="" type="checkbox"/> Allow lock screen control center	iOS 7+
<input checked="" type="checkbox"/> Allow lock screen notifications view	iOS 7+
<input checked="" type="checkbox"/> Allow lock screen today view	iOS 7+
<input checked="" type="checkbox"/> Allow OTAPKI updates	iOS 7+
<input checked="" type="checkbox"/> Allow app installation	
<input checked="" type="checkbox"/> Allow ui configuration profile installation	Supervised only
<input checked="" type="checkbox"/> Allow camera	
<input checked="" type="checkbox"/> Allow face time	
<input checked="" type="checkbox"/> Allow screen shot	
<input checked="" type="checkbox"/> Allow global background fetch when roaming	
<input checked="" type="checkbox"/> Allow assistant	
<input checked="" type="checkbox"/> Allow assistant while locked	
<input checked="" type="checkbox"/> Allow voice dialing	
<input checked="" type="checkbox"/> Allow passbook while locked	
<input checked="" type="checkbox"/> Allow in app purchases	
<input type="checkbox"/> Force iTunes store password entry	
<input checked="" type="checkbox"/> Allow multiplayer gaming	
<input checked="" type="checkbox"/> Allow game center	Supervised only
<input checked="" type="checkbox"/> Allow adding game center friends	
<input checked="" type="checkbox"/> Allow host pairing	iOS 7+ Supervised only
<input checked="" type="checkbox"/> Allow find my friends modification	iOS 7+ Supervised only
<input checked="" type="checkbox"/> Allow fingerprint for unlock	iOS 7+
<input checked="" type="checkbox"/> Allow account modification	iOS 7+ Supervised only
<input checked="" type="checkbox"/> Allow air drop	iOS 7+ Supervised only
<input checked="" type="checkbox"/> Force limit ad tracking	iOS 7+
<input checked="" type="checkbox"/> Allow assistant user generated content	iOS 7+ Supervised only

Restrictions Configuration – Table of Parameters		
Device Functionality		
Form Element	Type	Description
Allow lock screen control center	Checkbox	Select this option to allow Control Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow lock screen notifications view	Checkbox	Select this option to allow Notification Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow lock screen today view	Checkbox	Select this option to allow the Today View in Notification Center to be displayed in the lock screen. Note: This feature is available for iOS 7 and later versions.
Allow OTAPKI updates	Checkbox	Select this option to allow over-the-air public key infrastructure (OTAPKI) updates on devices. Note: This feature is available for iOS 7 and later versions.
Allow App Installation	Checkbox	Select this to allow the user to access App Store, iTunes and install or update apps. If left unchecked, the App Store icon is removed from the device's home screen and the user cannot access it.
Allow UI configuration profile installation	Checkbox	Selection this option to allow users to install UI configuration profile. Note: This option is available for supervised devices only.
Allow Camera	Checkbox	Select this to allow the user to take photos, videos or use FaceTime. If left unchecked, the camera icon is removed from the device and camera is disabled.
Allow FaceTime	Checkbox	Select this to allow the user to use FaceTime. The checkbox will be active only when 'Allow Camera' is enabled.
Allow Screen Shot	Checkbox	Select this to allow the user to take screenshots.
Allow Global Background Fetch When Roaming	Checkbox	Select this to allow the device when roaming to sync even when an account is not accessed by a user.
Allow Assistant	Checkbox	If enabled, users can use Siri, voice commands and dictation.
Allow Assistant While Locked	Checkbox	If enabled, users can use Siri even when the device is locked. The checkbox will be active only when 'Allow Assistant' is enabled.
Allow Voice Dialing	Checkbox	Select this to allow the user to dial their phone using voice commands.
Allow Passbook While Locked	Checkbox	If enabled, Passbook notifications will be displayed even when the device is locked.
Allow In App Purchases	Checkbox	Select this to allow the user to make in-app purchases
Force I Tunes Store Password Entry	Checkbox	If enabled, users have to enter their Apple ID password for making any purchase.
Allow Multiplayer Gaming	Checkbox	Select this to allow the user to play multiplayer game in Game Center.
Allow Game Center	Checkbox	If enable, users can access Game Center, an online multiplayer social gaming network. Note: This option is available for supervised devices only.

## Restrictions Configuration – Table of Parameters

Allow Adding Game Center Friends	Checkbox	If enabled, users can add friends in Game Center.
----------------------------------	----------	---

## Restrictions Configuration – Table of Parameters

Allow host pairing	Checkbox	Select this to allow host pairing on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
--------------------	----------	--




## Restrictions Configuration – Table of Parameters


Allow find my friends modification	Checkbox	Select this to enable Find My Friends on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
------------------------------------	----------	--

Restrictions Configuration – Table of Parameters		
Allow fingerprint for unlock	Checkbox	Select this to enable Touch ID to unlock devices. Note: This feature is available for iOS 7 and later versions.
Allow account modification	Checkbox	Select this to allow account modification on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Allow air drop	Checkbox	Select this to allow Air Drop on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Force limit ad tracking	Checkbox	Select this to limit ad tracking on devices. Note: This feature is available for iOS 7 and later versions.
Allow assistant user generated content	Checkbox	Select this to enable Siri to query user generated content from the Internet on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.

## Applications

 **Device functionality**  
Enable use of device features

---

 **Applications**  
Enable access to applications on the device

---

**Allow app cellular data modification** iOS 7+ Supervised only

---

**Allow open from managed to unmanaged** iOS 7+

---

**Allow open from unmanaged to managed** iOS 7+

---

**Allow you tube**

---

**Allow iTunes**

---

**Allow safari**

---

**Safari allow auto fill**

---

**Safari allow java script**

---


**Safari allow popups**

---

**Safari force fraud warning**

---



**Safari accept cookies**




Controls when Safari accepts cookies


---




**Autonomous single app mode permitted app IDs** iOS 7+ Supervised only



---

 [iCloud](#)

Restrictions Configuration – Table of Parameters		
Applications		
Form Element	Type	Description
Allow app cellular data modification	Checkbox	If enabled, users can make changes to cellular data usage for apps on devices. Note: This feature is available for iOS 7 and later versions and supervised devices only.
Allow open from managed to unmanaged	Checkbox	If enabled, users can send data from managed apps to unmanaged apps. Note: This feature is available for iOS 7 and later versions.
Allow open from unmanaged to managed	Checkbox	If enabled, users can send data from unmanaged apps to managed apps. Note: This feature is available for iOS 7 and later versions.
Allow You Tube	Checkbox	If enabled, users can access You Tube. If left unchecked, You Tube app is disabled and its icon removed from the home screen.
Allow i Tunes	Checkbox	If enabled, users can access iTune store. If left unchecked, iTune store is disabled and its icon removed from the home screen.
Allow Safari	Checkbox	Select this to allow the user to browse the Internet using Safari. If left unchecked, the Safari browser app is disabled and its icon removed from the home screen.
Safari Allow Auto Fill	Checkbox	If enabled, Safari will remember what users enter in web forms. The checkbox will be active only if the 'Allow Safari' checkbox is enabled.
Safari Allow Java Script	Checkbox	If enabled, Safari will support javascripts in websites. The checkbox will be active only if the 'Allow Safari' checkbox is enabled.
Safari Allow Popups	Checkbox	If enabled, Safari will allow pop ups to be displayed. The checkbox will be active only if the 'Allow Safari' checkbox is enabled.
Safari Force Fraud Warning	Checkbox	If enabled, Safari prevents user from visiting compromised or fraudulent websites.
Safari Accept Cookies	Drop-down	The drop-down will be active only when the 'Allow Safari' checkbox is enabled. The options available are: <ul style="list-style-type: none"> <li>• <b>Never</b> - Accept no cookies</li> <li>• <b>From visited sites</b> - Accept cookies only from visited websites</li> <li>• <b>Always</b> - Accept all cookies</li> </ul>
Autonomous single app mode permitted app IDs	Text Field	<p>Enter the app identifier in the field. The user will be able to see only the app entered in this field. You can also provide a variable in the field by clicking the  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>To remove the text field, click the  beside it.</p> <p>To add Autonomous single app mode permitted app IDs, click  button.</p>

Restrictions Configuration – Table of Parameters		
		Note: This feature is available for iOS 7 and later versions and supervised devices only.

## iCloud

**iCloud**  
Enable access to iCloud services

---

**Allow cloud keychain sync** iOS 7+

---

**Allow cloud backup**

---

**Allow cloud document sync**

---

**Allow photo stream**

---

**Allow shared stream**

---

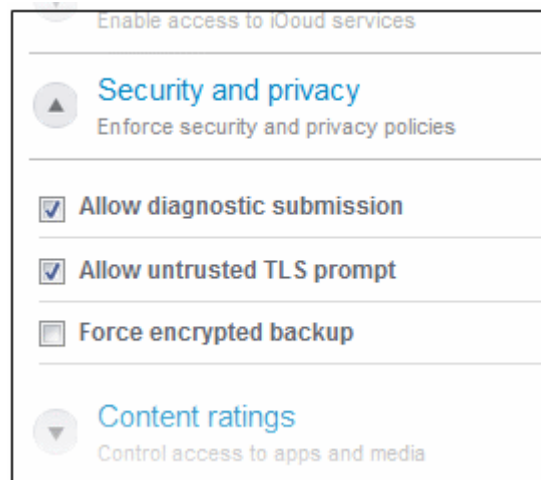
**Security and privacy**  
Enforce security and privacy policies

---

**Content ratings**  
Control access to apps and media

Restrictions Configuration – Table of Parameters		
iCloud		
Form Element	Type	Description
Allow cloud keychain sync	Checkbox	If enabled, users can sync Apple Keychain on iCloud on devices. Note: This feature is available for iOS 7 and later versions.
Allow Cloud Backup	Checkbox	If enabled, users can backup their device data to iCloud.
Allow Document Sync	Checkbox	If enabled, users can synchronize documents between iCloud and their device.
Allow Photo Stream	Checkbox	Users can use Photo Stream if this checkbox is enabled. If a profile with this restriction is applied to a device, Photo Stream photos will be removed from the device and no photos from Camera Roll will be uploaded to Photo Stream.
Allow Shared Stream	Checkbox	If enabled, users can share and view photos in Photo Stream.

## Security and Privacy



Restrictions Configuration – Table of Parameters		
Security and Privacy		
Form Element	Type	Description
Allow Diagnostic Submission	Checkbox	If enabled, iOS diagnostic information will be sent to Apple.
Allow Untrusted TLS Prompt	Checkbox	If enabled, users will be prompted if they want to trust unverified certificates. This settings applies to Calendar accounts, Contacts, Safari and to Mail.
Force Encrypted Backup	Checkbox	If left unchecked, in iTunes users have the option to encrypt or not encrypt backups from the device to a local computer. If this checkbox is enabled, in iTune users are forced to encrypt the backup.



## Content Ratings

**Security and privacy**  
Enforce security and privacy policies

---

**Content ratings**  
Control access to apps and media

---

**Allow explicit content**

---

**Allow iBookstore** Supervised only

---

**Allow iBookstore erotica** Supervised only

---

**Rating region**

Sets the region for the ratings

---

**Rating movies**

---

**Rating TV shows**

---

**Rating apps**

---

**Save**

Restrictions Configuration – Table of Parameters		
Content Ratings		
Form Element	Type	Description
Allow Explicit Content	Checkbox	If enabled, explicit content include music and video will be displayed in iTunes store instead being hidden. Content providers flag explicit content for easy identification.
Allow iBookstore	Checkbox	If enable, users can access iBookstore, an online bookstore from Apple. Note: This option is available for supervised devices only.
Allow iBookstore Erotica	Checkbox	If enabled, erotica books will be displayed in iBook store instead being hidden. Content providers flag explicit content for easy identification. Note: This option is available for supervised devices only.
Rating Region	Drop-down	Select a rating region from the drop-down.
Rating Movies	Drop-down	Select from the drop-down whether you want to allow or not allow movies or according to the ratings.
Rating TV Shows	Drop-down	Select from the drop-down whether you want to allow or not allow TV shows or according to the ratings.

**Restrictions Configuration – Table of Parameters**

Rating Apps	Drop-down	Select from the drop-down whether you want to allow or not allow Apps or allow according to the ratings.
-------------	-----------	--

- Click the 'Save' button after entering or selecting the parameters.



A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Restrictions section' button at the top.










**To configure Wi-Fi settings**

- Click anywhere on the 'Wi-Fi' row.

The settings screen for Wi-Fi will be displayed.

<ul style="list-style-type: none"> <li> <b>General</b> Configured</li> <li> <b>Passcode</b> Not configured</li> <li> <b>AirPlay</b> Not configured</li> <li> <b>AirPrint</b> Not configured</li> <li> <b>Restrictions</b> Not configured</li> <li> <b>Wi-Fi</b> Not configured</li> <li> <b>VPN</b> Not configured</li> <li> <b>Per-App VPN</b> Not configured</li> <li> <b>Mail</b> Not configured</li> <li> <b>Exchange ActiveSync</b> Not configured</li> <li> <b>LDAP</b> Not configured</li> <li> <b>Calendar</b> Not configured</li> <li> <b>Subscribed Calendars</b> Not configured</li> <li> <b>Contacts</b> Not configured</li> <li> <b>Global HTTP proxy</b> Not configured</li> <li> <b>Web Clip</b> Not configured</li> <li> <b>APN</b> Not configured</li> <li> <b>Cellular Networks</b> Not configured</li> <li> <b>Single Sign-On</b> Not configured</li> </ul>	<p><b>SSID *</b></p> <input type="text"/> <input type="button" value="↑↓"/> <p>Identification of the wireless network to connect to In iOS 7.0 and later, this is optional if a DomainName value is provided</p> <p><input type="checkbox"/> <b>Auto join</b> Automatically join the target network</p> <p><input type="checkbox"/> <b>Hidden network</b> Enable if the target network is not open or broadcasting</p> <p><b>Encryption type</b></p> <p>None <input type="button" value="v"/></p> <p>Wireless network encryption to use when connecting</p> <p><b>Proxy type</b></p> <p>None <input type="button" value="v"/></p> <p><b>Domain name</b> <span style="float: right;">iOS 7+</span></p> <input type="text"/> <input type="button" value="↑↓"/> <p><b>Displayed operator name</b> <span style="float: right;">iOS 7+</span></p> <input type="text"/> <input type="button" value="↑↓"/> <p><input type="checkbox"/> <b>Is hotspot</b> <span style="float: right;">iOS 7+</span></p> <p><input type="checkbox"/> <b>Service provider roaming enabled</b> <span style="float: right;">iOS 7+</span></p> <p><b>Roaming consortium ois</b> <span style="float: right;">iOS 7+</span></p> <input type="text"/> <input type="button" value="↑↓"/> <input type="button" value="-"/> <input type="text"/> <input type="button" value="+"/> <input type="text"/> <input type="button" value="↑↓"/> <input type="button" value="-"/> <input type="text"/> <input type="button" value="+"/> <b>NAI realm names</b> <span style="float: right;">iOS 7+</span> <input type="text"/> <input type="button" value="↑↓"/> <input type="button" value="-"/> <input type="text"/> <input type="button" value="+"/> <b>MCC and MNCs</b> <span style="float: right;">iOS 7+</span> <input type="text"/> <input type="button" value="↑↓"/> <input type="button" value="-"/> <input type="text"/> <input type="button" value="+"/> <p>Fields with * are required.</p> <p><input type="button" value="Save"/></p> <p><input type="button" value="Add new WiFi section"/></p>
--	--

Wi-Fi Settings – Table of Parameters		
Form Element	Type	Description
SSID	Text Field	Enter a unique identifier (Service Set Identifier) of a wireless network that a device should connect to. Note: In iOS 7 and later versions, this is optional if Domain Name is provided.
Auto Join	Checkbox	If enabled, devices will automatically connect to the configured wireless network.
Hidden Network	Checkbox	Specify whether the wireless network is hidden or not.
Encryption Type	Drop-down	Select the type of encryption used by the wireless network from the drop-down. The options available are: <ul style="list-style-type: none"> <li>• None</li> <li>• WEP</li> <li>• WPA / WPA2</li> <li>• Any (Personal)</li> <li>• WEP Enterprise</li> <li>• WPA / WPA2 Enterprise</li> <li>• Any (Enterprise)</li> </ul> The Password field will appear if any of the options, WEP, WPA / WPA2 and Any (Personal) are chosen. If any of the Enterprise is chosen, then select the supported protocols and configure authentication. The options available are: TLS, LEAP, TTLS, PEAP, EAP-FAST, EAP-SIM, Use Pac and Provision Pac Anonymously.
Password	Text Field	Leave the field blank. The user will be prompted to enter the password while accessing the Wi-Fi network.
Proxy Type	Drop-down	Select the proxy settings for the wireless network from the drop-down. The options available are: <ul style="list-style-type: none"> <li>• None</li> <li>• Manual</li> <li>• Auto</li> </ul> If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields. If you select 'Auto', enter the URL of the Proxy Pac.
Domain Name	Text Field	Enter the domain name used for Wi-Fi hotspot 2.0 which the devices will connect to. This is optional and can be provided instead of Service Set Identifier. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> . Note: This feature is available for iOS 7 and later versions.
Displayed Operator Name	Text Field	Enter the network operator name that will be displayed in the devices. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> . Note: This feature is available for iOS 7 and later versions.

Wi-Fi Settings – Table of Parameters		
Is Hotspot	Checkbox	If enabled, the network is treated as a hotspot. Note: This feature is available for iOS 7 and later versions.
Service Provider Roaming Enabled	Checkbox	If enabled, devices can connect to roaming service providers. Note: This feature is available for iOS 7 and later versions.
Roaming Consortium Ols	Text Field	<p>Enter the Roaming Consortium Organization Identifier of the service provider to which the devices will connect to. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>To removed the field, click the  button beside it.</p> <p>Click the  button to add Roaming Consortium Ols fields.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
NAI Realm Names	Text Field	<p>Enter the Network Access Identifier (NAI) realm names used for Wi-Fi hotspot 2.0. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>To remove the field, click the  beside it.</p> <p>Click the  button to add more NAI Realm Names.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
MCC and MNCs	Text Field	<p>Enter the Mobile Country Code (MCC) / Mobile Network Code (MNC) pairs used for Wi-Fi hotspot 2.0. Each string should contain exactly 6 digits. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>To remove the field, click the  beside it.</p> <p>Click the  button to add more MCC and MNCs.</p> <p>Note: This feature is available for iOS 7 and later versions.</p>
















- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Wi-Fi section' button at the top.


## To configure VPN settings

- Click anywhere on the 'VPN' row.




The settings screen for VPN will be displayed.







<ul style="list-style-type: none"> <li> <b>General</b> Configured</li> <li> <b>Passcode</b> Not configured</li> <li> <b>AirPlay</b> Not configured</li> <li> <b>AirPrint</b> Not configured</li> <li> <b>Restrictions</b> Not configured</li> <li> <b>Wi-Fi</b> Not configured</li> <li style="background-color: #e0e0e0;"> <b>VPN</b> Not configured</li> <li> <b>Per-App VPN</b> Not configured</li> <li> <b>Mail</b> Not configured</li> <li> <b>Exchange ActiveSync</b> Not configured</li> <li> <b>LDAP</b> Not configured</li> <li> <b>Calendar</b> Not configured</li> <li> <b>Subscribed Calendars</b> Not configured</li> <li> <b>Contacts</b> Not configured</li> <li> <b>Global HTTP proxy</b> Not configured</li> </ul>	<p><b>User name</b></p> <input type="text"/> <p>Display name of the connection (displayed on the device)</p> <p><b>Connection type *</b></p> <p>L2TP</p> <p>The type of connection enabled by this policy</p> <p><input type="checkbox"/> <b>Override primary</b></p> <p><b>Server *</b></p> <input type="text"/> <p>Hostname or IP address for server</p> <p><b>Account</b></p> <input type="text"/> <p>User account for authenticating the connection</p> <p><b>User Authentication</b></p> <p><input type="radio"/> Password</p> <p><input type="radio"/> RSA SecurID</p> <p>Authentication type for connection</p> <p><b>Shared secret</b></p> <input type="text"/> <p>Shared secret for the connection</p> <p><b>Proxy type</b></p> <p>None</p> <p>Fields with * are required.</p> <p><input type="button" value="Save"/></p> <p><input type="button" value="Add new VPN section"/></p>
---	--










VPN Settings – Table of Parameters		
Form Element	Type	Description
User Name	Text Field	Enter the name of the connection, which will be displayed on the device. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Connection Type	Drop-down	Select the VPN connection type from drop-down. The options available are: L2TP, PPTP, IPSec (Cisco), CISCO AnyConnection, Juniper SSL, F5 SSL and OpenVPN. The settings for each type is explained in the next table, <b>VPN connection type settings</b> .
Proxy	Drop-down	Select the proxy settings for the VPN from the drop-down. The options available are: <ul style="list-style-type: none"> <li>• None</li> <li>• Manual</li> <li>• Auto</li> </ul> <p>If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields.</p> <p>If you select 'Auto', enter the URL of the Proxy Pac.</p>


## VPN Connection Type settings

VPN Connection Type Settings – Table of Parameters	
Connection Type	Description
L2TP	<ul style="list-style-type: none"> <li>• Override Primary – Enable this to override the primary server.</li> <li>• Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>• Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>• User Authentication – If Password is selected, then the user should enter the password and the secret pin in the respective fields. If RSA SecurID is selected, then the user should enter the secret pin provided by the administrator.</li> </ul>
PPTP	<ul style="list-style-type: none"> <li>• Override Primary – Enable this to override the primary server.</li> <li>• Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section</li> </ul>

VPN Connection Type Settings – Table of Parameters	
	<p><b>Configuring Custom Variables.</b></p> <ul style="list-style-type: none"> <li>Account – Enter the VPN account name. You can also provide a variable in the field  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>User Authentication – If Password is selected, then the user should enter the password and the secret pin in the respective fields. If RSA SecurID is selected, then the user should enter the secret pin provided by the administrator.</li> <li>Encryption Level – Select the encryption level from the drop-down. The options available are, None, Automatic and Maximum (128 bit).</li> </ul>
IPSec (Cisco)	<ul style="list-style-type: none"> <li>Override Primary – Enable this to override the primary server.</li> <li>Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>Password – The user should enter the password for the account.</li> <li>Authentication Method - Select the authentication method from the drop-down either Shared secret / Group name or Certificate. If the former is selected, then the user should enter the Group name and secret pin in the respective fields. If the later method is selected, then make sure certificate in the device and the server are valid and the server is configured to identify the users based on fields in the client certificate.</li> </ul>
Cisco AnyConnection	<ul style="list-style-type: none"> <li>Override Primary – Enable this to override the primary server.</li> <li>Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>Group – Enter the group name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables.</b></li> <li>User Authentication – Two options are available, Password and Certificate. If password is selected, then the user should enter the authorization password in the field. If Certificate is selected, then make sure certificate in the device and the server are valid and the server is configured to identify the users based on fields in</li> </ul>

VPN Connection Type Settings – Table of Parameters	
	the client certificate.
Juniper SSL	<ul style="list-style-type: none"> <li>Override Primary – Enable this to override the primary server.</li> <li>Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>Realm – Enter the name of the authentication server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>Role – Enter the role of the user. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>User Authentication – Two options are available, Password and Certificate. If password is selected, then the user should enter the authorization password in the field. If Certificate is selected, then make sure certificate in the device and the server are valid and the server is configured to identify the users based on fields in the client certificate.</li> </ul>
F5 SSL	<ul style="list-style-type: none"> <li>Override Primary – Enable this to override the primary server.</li> <li>Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>User Authentication – Two options are available, Password and Certificate. If password is selected, then the user should enter the authorization password in the field. If Certificate is selected, then make sure certificate in the device and the server are valid and the server is configured to identify the users based on fields in the client certificate.</li> </ul>
OpenVPN	<ul style="list-style-type: none"> <li>Override Primary – Enable this to override the primary server.</li> <li>Server – Enter IP address of the primary server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> </ul>

## VPN Connection Type Settings – Table of Parameters

	<ul style="list-style-type: none"> <li>Account – Enter the VPN account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</li> <li>User Authentication – Two options are available, Password and Certificate. If password is selected, then the user should enter the authorization password in the field. If Certificate is selected, then make sure certificate in the device and the server are valid and the server is configured to identify the users based on fields in the client certificate.</li> </ul>
--	--

- Click the 'Save' button after entering or selecting the parameters.




A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete VPN section' button at the top.

### To configure Per-App VPN settings

If you would like to connect only certain apps to connect via VPN, then this feature allows you to configure the settings. This feature is available for iOS 7 and later versions.

- Click anywhere on the 'Per-APP VPN' row.

The settings screen for Per-App VPN will be displayed.

- **Automatically start Per-App VPN connection** – Select this checkbox if the per-app VPN connection should start automatically when the app starts.
- **Safari domains** – Enter the domain that will trigger this VPN connection in Safari. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section **Configuring Custom Variables**. Click the  button to add more domains in the field. If you want to remove a domain from the list, click the  button beside it.

For details on other settings please refer to the section '**To configure VPN settings**'.

- Click the 'Save' button after entering or selecting the parameters.


A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Per-App VPN section' button at the top.

## To configure Mail settings

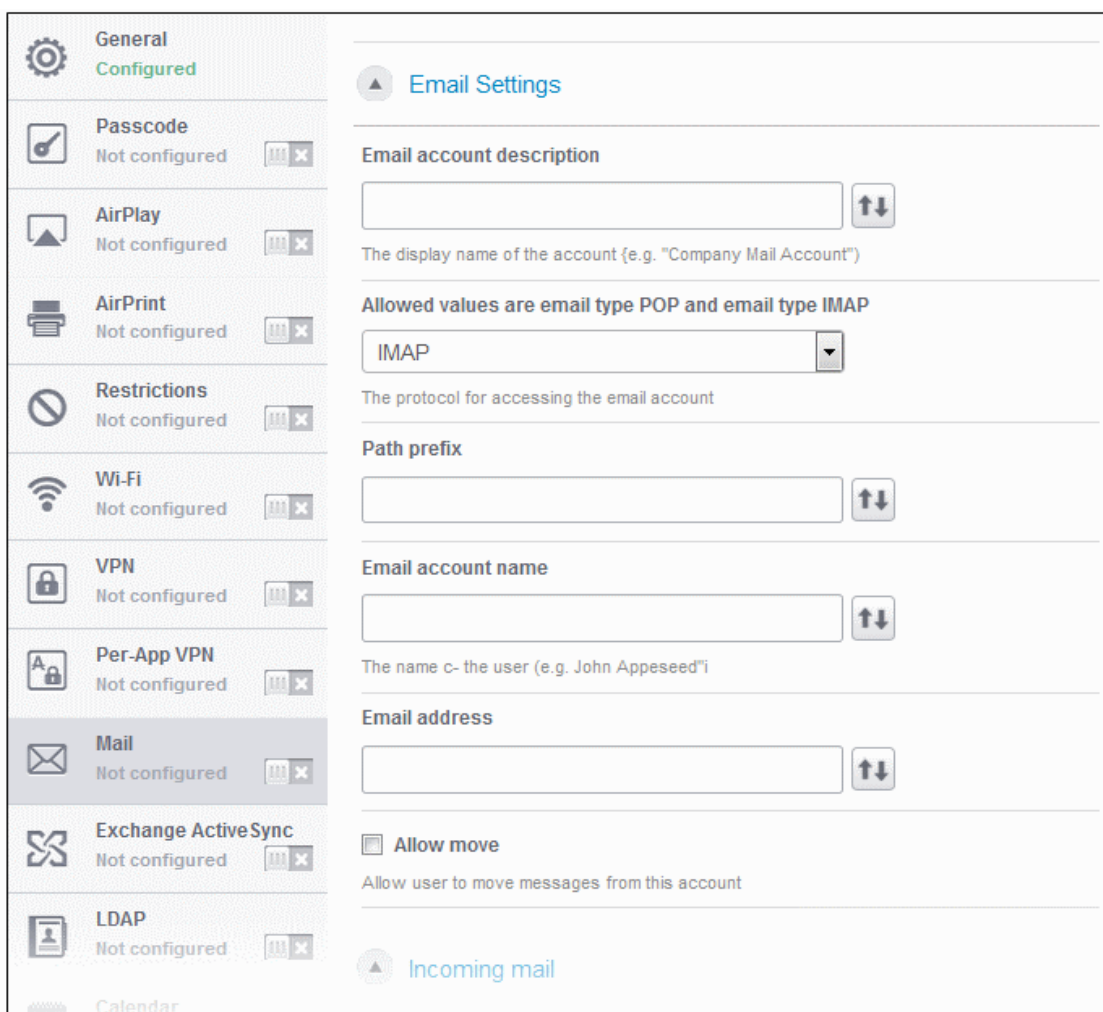
- Click anywhere on the 'Mail' row.

The settings screen for Mail will be displayed. It is divided into three main sections:

- **Email Account Details**
- **Incoming Mail**
- **Outgoing Mail**

You can expand/collapse a section by clicking the  button beside each section head.

## Email Account Details







The screenshot shows the 'Email Settings' configuration screen. On the left is a sidebar menu with various system settings, where 'Mail' is currently selected and highlighted. The main content area is titled 'Email Settings' and contains the following fields and options:

- Email account description:** A text input field with an expand/collapse button (↑↓).
- Allowed values are email type POP and email type IMAP:** A dropdown menu currently set to 'IMAP'.
- Path prefix:** A text input field with an expand/collapse button (↑↓).
- Email account name:** A text input field with an expand/collapse button (↑↓).
- Email address:** A text input field with an expand/collapse button (↑↓).
- Allow move:** A checkbox that is currently checked, with the label 'Allow user to move messages from this account' below it.

At the bottom of the main content area, there is a section header for 'Incoming mail' with an expand/collapse button (↑).



Mail Account Settings – Table of Parameters		
Email Account Details		
Form Element	Type	Description
Email Account Description	Text Field	Enter a description for the email account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Allowed values for Email Type	Drop-down	Select IMAP or POP from the email type for the profile.
Path prefix	Text Field	This will be visible if IMAP is chosen as Email Type in the previous step. Enter the path of the inbox in the field. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Email Account Name	Text Field	Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Email Address	Text Field	Click the Insert Variable button  beside the field, select '%u.mail%' from the 'Variables list' and click 'Apply'. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Allow move	Checkbox	If enabled, the user can move sent or received mails to another account.

## Incoming Mail Settings

**▲ Incoming mail**

---

**Designates the incoming mail server host name (or IP address) \***

↑↓

Hostname or IP address, and port number for incoming mail

---

**Designates the incoming mail server port number \***

↑↓

---

**Incoming mail server username**

↑↓

The username used to connect to the server for incoming mail

---

**Allowed values are email auth password and email auth none**

▼

The authentication method for the incoming mail server

---

**Incoming password**

↑↓

Password for the incoming mail server

---

**Incoming mail server use SSL**

Retrieve incoming mail through secure socket layer



---


**▼ Outgoing mail**

---

Fields with \* are required.

Save

Mail Account Settings – Table of Parameters		
Incoming Email Settings		
Form Element	Type	Description
Designates the incoming mail server host name (or IP address)	Text Field	Enter the host name of the incoming mail server or its IP address . You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Designates the incoming mail server port number	Text Field	Enter the server port number used for incoming mail service. For POP3, it is usually 110 and if SSL is enabled it is 995. For IMAP, it is usually 143 and if SSL is enabled it is 993. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .

Mail Account Settings – Table of Parameters		
Incoming Mail Server Username	Text Field	<p>Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p>
The Authentication Method for the Incoming Mail Server	Drop-down	<p>Select the type of authentication method for mail account from the drop-down. The options available are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Password</li> <li>• MD5 Challenge-Response</li> <li>• NTLM</li> <li>• HTTP MD5 Digest</li> </ul>
Incoming Password	Text Field	<p>Leave the field blank. If authentication is chosen in the previous step, then user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.</p>
Incoming Mail Server Use SSL	Checkbox	<p>If enabled, communication between incoming mail server and devices is encrypted using SSL.</p>

## Outgoing Mail Settings

▲ **Outgoing mail**

---

**outgoing mail server host name \***

Hostname or IP address, and port number for outgoing mail

---

**Designates the outgoing mail server port number. If no port number is specified, ports 25, 587 and 465 are used, in this order \***

---

**Outgoing mail server username**

The username used to connect to the server for outgoing mail

---

**outgoing mail server authentication**

The authentication method for the outgoing mail server

---

**Outgoing password**

Password for the outgoing mail server

---

**Outgoing password same as incoming password**  
SMTP authentication uses the same password as POP/IMAP

---

**Disable mail recents syncing**  
Include this account in recent address syncing

---

**Prevent app sheet**  
Send outgoing mail from this account only from Mail app

---




**Outgoing mail server use SSL**  
Send outgoing mail through secure socket layer

---

**SMIME enabled**  
Send outgoing mail using S/MIME encryption

---

Fields with \* are required.

Mail Account Settings – Table of Parameters		
Outgoing Email Settings		
Form Element	Type	Description
Outgoing Mails Server Host Name	Text Field	Enter the host name or IP address for the outgoing mail server. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Designates the outgoing mail server port number	Text Field	Enter the server port number used for outgoing mail service. If no port number is specified then ports 25, 587 and 465 are used in the given order. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Outgoing Mail Server Username	Text Field	Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <a href="#">Configuring Custom Variables</a> .
Outgoing Mail Server Authentication	Drop-down	Select the type of authentication method for outgoing mail server from the drop-down. The options available are: <ul style="list-style-type: none"> <li>• None</li> <li>• Password</li> <li>• MD5 Challenge-Response</li> <li>• NTLM</li> <li>• HTTP MD5 Digest</li> </ul>
Outgoing Password	Text Field	Leave the field blank. If authentication is chosen in the previous step, then user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Outgoing Password Same as Incoming Password	Checkbox	If enabled, the password for incoming will be used for outgoing also.
Disable Mail Recents Syncing	Checkbox	If enabled, recently used emailed addresses are not synced with other devices via iCloud.
Prevent App Sheet	Checkbox	If enabled, outgoing mails can be sent from this account only via mail app.
Outgoing Mail Server Use SSL	Checkbox	If enabled, communication between outgoing mail server and devices is encrypted using SSL.
Smime Enabled	Checkbox	If enabled, users can sign and encrypt email messages from their devices. Please note that certificates have to be installed in users' devices before this feature can be used.

- Click 'Add New Mail section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the

parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Mail section' button at the top.

## To configure Exchange ActiveSync settings

- Click anywhere on the 'Exchange ActiveSync' row.

The settings screen for Exchange ActiveSync will be displayed.

**General**  
Configured

**Passcode**  
Not configured

**AirPlay**  
Not configured

**AirPrint**  
Not configured

**Restrictions**  
Not configured

**Wi-Fi**  
Not configured

**VPN**  
Not configured

**Per-App VPN**  
Not configured

**Mail**  
Not configured

**Exchange ActiveSync**  
Not configured

**LDAP**  
Not configured

**Calendar**  
Not configured

**Subscribed Calendars**  
Not configured

**Contacts**  
Not configured

**Global HTTP proxy**  
Not configured

**Web Clip**  
Not configured

**APN**  
Not configured

**Cellular Networks**  
Not configured

**Single Sign-On**  
Not configured

**Account Name**  
Name for the Exchange ActiveSync account

**Exchange ActiveSync Host \***  
Microsoft Exchange Server

**Allow Move**  
Allow user to move messages from this account

**Disable mail recent syncing**  
Include this account in recent address syncing

**Prevent app sheet**  
Send outgoing mail from this account only from Mail app

**Use SSL**  
Send all communication through secure socket layer

**S/MIME enabled**  
Send outgoing mail using S/MIME encryption

**Domain**  
Domain for the account.

**Username**  
User for the account.

**Email Address**  
The address of the account (e.g. "john@comodo.com").

**Password**  
The password for the account (e.g. "MyMsswOrd").






**Past days of mail to sync**  
The number of past days of mail to sync

**Certificate**  
None

Upload a file

Fields with \* are required.

Save

Exchange ActiveSync Settings – Table of Parameters		
Form Element	Type	Description
Account Name	Text Field	Enter the Exchange ActiveSync account name. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Exchange ActiveSync host	Text Field	Enter the Exchange host name (Microsoft Exchange Server). You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Allow move	Checkbox	If enabled, the user can move sent or received mails to another account.
Disable Mail Recent Syncing	Checkbox	If enabled, recently used emailed addresses are not synced with other devices via iCloud.
Prevent App Sheet	Checkbox	If enabled, mails cannot be sent using third-party applications.
Use SSL	Checkbox	If enabled, communication between Exchange server and devices will be encrypted using SSL.
Smime Enabled	Checkbox	If enabled, users can sign and encrypt email messages from their devices. Please note that certificates have to be installed in users' devices before this feature can be used.
Domain	Text Field	Address of the account. Click the Insert Variable button  beside the field, select '%u.mail%' from the 'Variables list' and click 'Apply'. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
User Name	Text Field	User name for the account. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Email Address	Text Field	Address of the account. Click the Insert Variable button  beside the field, select '%u.mail%' from the 'Variables list' and click 'Apply'. The email address of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Password	Text Field	Leave the field blank. The user will be prompted to enter the password while configuring the email account for the first time. After it is validated, the users can access the email account without entering the password.
Past days of mail to sync	Drop-down	Select from the drop-down the period for which mail sync will be active. The options range from One day to Unlimited.
Certificate	Drop-down	Select the SSL certificate from the drop-down or click the 'Upload a file' to upload a certificate.

- Click the 'Save' button after entering or selecting the parameters.



A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Exchange ActiveSync section' button at the top.





## To configure LDAP settings

- Click anywhere on the 'LDAP' row.

The settings screen for LDAP will be displayed.

The screenshot displays the LDAP configuration interface. On the left is a sidebar with settings: General (Configured), Passcode (Not configured), AirPlay (Not configured), AirPrint (Not configured), Restrictions (Not configured), Wi-Fi (Not configured), VPN (Not configured), Per-App VPN (Not configured), Mail (Not configured), Exchange ActiveSync (Not configured), **LDAP (Not configured)**, Calendar (Not configured), Subscribed Calendars (Not configured), and Contacts. The main configuration area includes:

- Account Description:** A text input field with a swap icon.
- Account Hostname \*:** A text input field with a swap icon. Below it is the text: "The LDAP hostname or IP address".
- Account Username:** A text input field with a swap icon. Below it is the text: "The username for this LDAP account".
- Account Password:** A text input field with a swap icon. Below it is the text: "The password for this LDAP account".
- Use SSL:** A checkbox labeled "Use SSL" with the text "Enable Secure Socket Layer for this connection" below it.
- Search Settings:** A table with columns "Description", "Scope", and "Search base". The "Scope" column has a dropdown menu set to "Base". The "Search base" column has an empty text input field with a red "X" icon to its right.
- Results per page:** A dropdown menu set to "20" with a "+" icon to its right.
- Search settings for this LDAP server:** A text input field.
- Fields with \* are required.**
- Save:** A button at the bottom.

LDAP Settings – Table of Parameters		
Form Element	Type	Description
Account Description	Text Field	Enter the display name of the LDAP account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Host Name	Text Field	Enter the LDAP hostname or IP address. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account User Name	Text Field	The username for the LDAP account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Password	Text Field	The password for the LDAP account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Use SSL	Checkbox	If enabled, the communication will be encrypted.

## Searching the LDAP directory

Admins can search for email contacts in the domain using the search feature.

Use SSL  
Enable Secure Socket Layer for this connection

---

**Search Settings**

Description	Scope	Search base
<input style="width: 90%;" type="text"/>	<div style="border: 1px solid #ccc; padding: 2px;">                     Base ▼                 </div> <div style="border: 1px solid #ccc; padding: 2px; background-color: #e0e0e0;">                     Base                 </div> <div style="border: 1px solid #ccc; padding: 2px;">                     One level Subtree                 </div>	<input style="width: 90%;" type="text"/> <span style="color: red; font-weight: bold;">✘</span>



Results per page:

Search settings for this LDAP server

Fields with \* are required.

LDAP Search Settings – Table of Parameters		
Form Element	Type	Description

LDAP Search Settings – Table of Parameters		
Description	Text Field	Enter the name of the search
Scope	Drop-down	Select from the drop-down to what level in the LDAP tree structure the search should run. Base - Searches only the defined search base. One level - Searches the base and the first level below it. Subtree - Searches the base and all the levels below it.
Search base	Text Field	Enter the search base for which the search will be restricted. For example, you might want to allow users to search only for other email users via LDAP.

- You can add more Search Settings by clicking the  below.
- Select the number of results to be displayed from the 'Results per page' from the drop-down.
- To remove a search item, click the  button at the far end of the row.
- Click 'Add new LDAP section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Profile successfully updated' will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete LDAP section' button at the top.

## To configure Calendar settings

- Click anywhere on the 'Calendar' row.

The settings screen for CalDav will be displayed.

- General**  
Configured
- Passcode**  
Not configured
- AirPlay**  
Not configured
- AirPrint**  
Not configured
- Restrictions**  
Not configured
- Wi-Fi**  
Not configured
- VPN**  
Not configured
- Per-App VPN**  
Not configured
- Mail**  
Not configured
- Exchange ActiveSync**  
Not configured
- LDAP**  
Not configured
- Calendar**  
Not configured
- Subscribed Calendars**  
Not configured
- Contacts**  
Not configured

**Account Description**

The display name of the account (e.g. "Company CalDAV Account")

**Account Hostname \***

The CalDAV hostname or IP address and port number

**Account Port \***

**CalDAV Account**

The CalDAV username

**Account Password**

The CalDAV password

**Use SSL**  
Enable Secure Socket Layer communication with CalDAV server

**Principal URL**




The Principal URL for the CalDAV account

Fields with \* are required.

Calendar Settings – Table of Parameters		
Form Element	Type	Description
Account Description	Text Field	Enter the display name of the CalDav account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Host Name	Text Field	Enter the CalDav host name or IP address. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Port	Text Field	Enter the port number on which to connect to the server. You can also provide a

Comodo Mobile Device Manager - Administrator Guide | © 2014 Comodo Security Solutions Inc. | All rights reserved

97

Calendar Settings – Table of Parameters		
		variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
CalDav Account	Text Field	The user name of the CalDav user. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Password	Text Field	The password for the CalDav account. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, the users can access the account without entering the credentials.
Use SSL	Checkbox	If enabled, SSL connection will be established with the CalDav server.
Principal URL	Text Field	Enter the Principal URL of the CalDav account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .

- Click 'Add new Calendar section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Calendar section' button at the top.




## To configure Subscribed Calendar settings

- Click anywhere on the 'Subscribed Calendars' row.

The settings screen for Subscribed Calendar will be displayed.

The screenshot displays the configuration page for 'Subscribed Calendars'. The left-hand navigation pane lists various system settings, with 'Subscribed Calendars' currently selected. The main configuration area includes the following elements:

- Description:** A text input field with an 'Insert Variable' button (up/down arrows) to its right. Below the field is the text: 'The description of the calendar subscription'.
- URL \*:** A text input field with an 'Insert Variable' button. Below the field is the text: 'The URL of the calendar file'.
- Username:** A text input field with an 'Insert Variable' button. Below the field is the text: 'The usemame for this subscription'.
- Password:** A text input field with an 'Insert Variable' button. Below the field is the text: 'The password for this subscription'.
- Use SSL:** A checkbox.
- Fields with \* are required.**
- Save:** A button to save the configuration.
- Add new Subscribed calendar section:** A button to add a new calendar entry.

Subscribed Calendars Settings – Table of Parameters		
Form Element	Type	Description
Description	Text Field	Enter the description of the calendar subscription. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
URL	Text Field	Enter the URL of the subscribed calendar file. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Username	Text Field	The user name for the subscription. Click the Insert Variable button 



Subscribed Calendars Settings – Table of Parameters		
		beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Password	Text Field	The password for the subscription. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, the users can access the account without entering the credentials.
Use SSL	Checkbox	If enabled, SSL connection will be established with the server.

- Click 'Add new Subscribed calendar section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.



A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Subscribed Calendar section' button at the top.



### To configure Contacts settings

- Click anywhere on the 'Contacts' row.

The settings screen for Contacts will be displayed.



Contacts Settings – Table of Parameters		
Form Element	Type	Description
Account Description	Text Field	Enter the display name of the CardDav account. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Host Name	Text Field	Enter the CardDav host name or IP address. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Port	Text Field	Enter the port number on which to connect to the server. You can also provide a

Contacts Settings – Table of Parameters		
		variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Username	Text Field	The user name of the CardDav user. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Account Password	Text Field	The password for the CardDav account. Leave the field blank. The user will be prompted to enter the password while configuring the account for the first time. After it is validated, the users can access the account without entering the password.
Use SSL	Checkbox	If enabled, SSL connection will be established with the CardDav server.
Principal URL	Text Field	Enter the Principal URL of the CardDav account.

- Click 'Add new Contacts section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now.

## To configure Global HTTP proxy settings

This feature is available for Supervised devices only.

- Click anywhere on the 'Global HTTP proxy' row.


The settings screen for Global HTTP Proxy will be displayed.

Supervised only

**Proxy type**

Manual


**Proxy server**



Fully qualified address and port of the proxy server


---

**Proxy server port**



---


**Proxy username**



Username used to connect to the proxy server



---

**Proxy password**



Password used when connecting to the proxy

---

Global HTTP Proxy Settings – Table of Parameters		
Form Element	Type	Description
Proxy	Drop-down	<p>Select the proxy settings for the VPN from the drop-down. The options available are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Manual</li> <li>• Auto</li> </ul> <p>If you select 'Manual', enter the IP address of the proxy server, proxy server port, proxy username and proxy password in the respective fields. You can also provide a variable in the respective fields by clicking the Insert Variable button  beside them, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p> <p>If you select 'Auto', enter the URL of the Proxy Pac. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b>.</p>

- Click the 'Save' button after entering or selecting the parameters.


A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Global HTTP Proxy section' button at the top.

## To configure Web Clip settings

- Click anywhere on the 'Web Clip' row.


The settings screen for Web Clip will be displayed.

**Label \***

   
The name to display for the Web Clip

---

**URL \***


   
The URL to be displayed when selecting the Web Clip

---

**Removable**

Enable removal of the Web Clip

---



The icon used for the web clip

---

**Precomposed**

The icon will be displayed with no added visual effects

---



**Full screen**

Controls whether the web clip launches as a Full Screen application

---

Fields with \* are required.

**Web Clip Settings – Table of Parameters**

Form Element	Type	Description
Label	Text Field	Enter the display name of the Web Clip. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
URL	Text Field	Enter the URL to be displayed when Web Clip is opened. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Removable	Checkbox	If enabled, users can remove the Web Clip from their devices.
Upload a file	Button	Upload the image to be used as icon for Web Clip.
Precomposed	Checkbox	If enabled, the Web Clip icon will be displayed with no added visual effects.
Full Screen	Checkbox	If enabled, the Web Clip will be displayed as a full screen application.

## Web Clip Settings – Table of Parameters

--	--	--

- Click 'Add new Web Clip section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Web Clip section' button at the top.

### To configure APN settings

**Note:** The APN settings is deprecated in favor of the Cellular settings in iOS 7 and later versions.

- Click anywhere on the 'APN' row.

The settings screen for APN will be displayed.

In iOS 7 and later, the APN payload is deprecated in favor of the Cellular payload.

---

**Access Point Name (APN) \***

  
The name of the carrier (GPRS) access point

---

**Access Point User Name**

  
The user name to connect to the access point

---

**Access Point Password**

  
The password to connect to the access point

---






**Proxy Server**

  
The fully qualified address and port of the proxy server

---

**Proxy Port**

  
Fields with \* are required.

APN Settings – Table of Parameters		
Form Element	Type	Description
Access Point Name (APN)	Text Field	Enter the name of the GPRS access point provided by the carrier. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Access Point User Name	Text Field	Enter the username to connect to the access point. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Password	Text Field	The password to connect to the access point. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Proxy Server	Text Field	Enter the proxy host settings provided by the carrier. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Proxy Port	Text Field	Enter the port number of the proxy host provided by the carrier. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .

- Click the 'Save' button after entering or selecting the parameters.

A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete APN section' button at the top.


### To configure Cellulars settings

**Note:** A cellular setting cannot be installed if an APN setting is already installed. This feature is available for iOS 7 and later versions only.

- Click anywhere on the 'Cellulars' row.


The settings screen for Cellulars will be displayed.

**Name \*** iOS 7+


---

**Authentication type** iOS 7+

CHAP 


---

**Username** iOS 7+

---


**Password** iOS 7+


---

**APNs** iOS 7+


**Name \*** ×


**Username**


**Authentication type**

CHAP 


**Password**


  


**Proxy server**

**Proxy port**











---

Fields with \* are required.

**Save**

**Add new Cellular section**



Cellular Settings – Table of Parameters		
Form Element	Type	Description
Name	Text Field	Enter the name for this configuration. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Authentication Type	Drop-down	Select the authentication type from the drop-down. The options are CHAP or PAP.
Username	Text Field	Enter the user name used for authentication. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Password	Text Field	Enter the password used for authentication. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
APNs		
Name	Text Field	Enter the name for this configuration. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Username	Text Field	Enter the user name used for authentication. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Authentication Type	Drop-down	Select the authentication type from the drop-down. The options are CHAP or PAP.
Password	Text Field	Enter the password used for authentication. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Proxy Server	Text Field	Enter the proxy server's network address. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Proxy Port	Text Field	Enter the proxy server's port. You can also provide a variable in the field by clicking the Insert Variable button  beside it, select the variable from the list and click Apply. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .

Cellular Settings – Table of Parameters	
	Click '+' to add more APN sections. To remove a section, click the 'x' sign beside the Name field of an APN.

- Click 'Add new Cellular section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.

A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Cellular Networks section' button at the top.

### To configure Single Sign-On settings

This settings is used to configure Kerberos authentication process and is available in iOS 7 or later versions only.

- Click anywhere on the 'Cellulars' row.

The settings screen for Single Sign-On will be displayed.

**Name \***
iOS 7+

---

**Principal name**
iOS 7+

---

**Realm \***
iOS 7+

---

**URL Prefix Matches**
iOS 7+

---

**App Identifier Matches**
iOS 7+

---

Fields with \* are required.

Save

Add New Single Sign-On Section

Single Sign-On Settings – Table of Parameters		
Form Element	Type	Description
Name	Text Field	Enter the name for the account. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Principal Name	Text Field	Enter the Kerberos principal name. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
Realm	Text Field	Enter the Kerberos realm name in proper capitals. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .
URL prefix matches	Text Field	Enter the URL prefix, which must be matched in order to use this account for Kerberos authentication over HTTP. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .  Click '+' button to add more 'URL prefix matches' fields. To remove a URL prefix, click the minus (-) button beside it.
App identifier matches	Text Field	Enter the bundle ID of apps that are allowed to use this login. If this field is left blank, this login matches all app IDs. Click the Insert Variable button  beside the field, select '%u.login%' from the 'Variables list' and click 'Apply'. The Usernames of the users to whom the profile is associated will be automatically filled. For more details on variables, refer to the section <b>Configuring Custom Variables</b> .  Click '+' button to add more 'App identifier matches' fields. To remove an App identifier match, click the minus (-) button beside it.

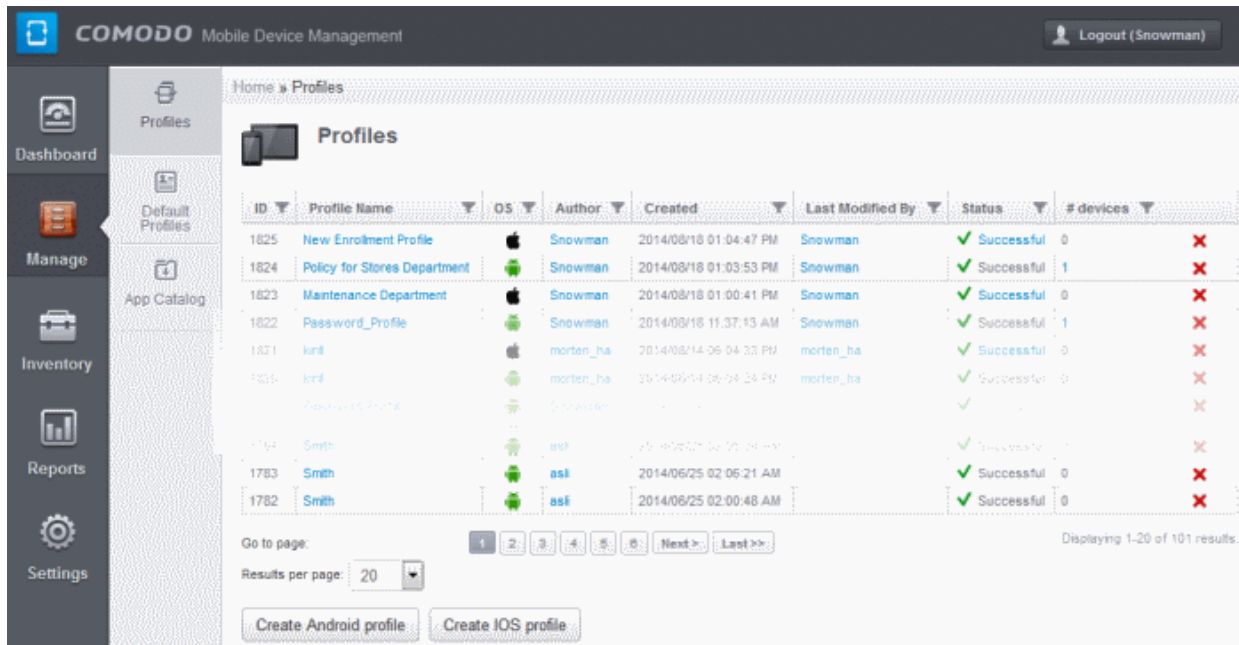
- Click 'Add new Single Sign-On section' to include another section in the screen.
- Click the 'Save' button after entering or selecting the parameters.


A message 'Sub profile' successfully saved will be displayed and the 'Configured' button in the row will turn green indicating the parameters for it is set now. The setting for the profile can be enabled or disabled by using the toggle switch beside it. If you want to remove the setting permanently for the profile, then click the 'Delete Single Sign-on section' button at the top.

## 4.2. Viewing the Profiles

Profiles that are created for both iOS and Android devices are listed in the 'Profiles' interface. The screen also allows an administrator to create a new profile.


To open the Profiles interface, click the 'Manage' tab from the left hand side navigation and choose 'Profiles' from the options.

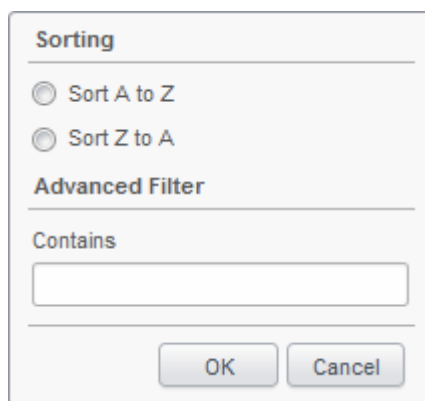


Profiles - Column Descriptions		
Column Heading	Description	
ID	The Unique ID number assigned to the profile.	
Profile Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section <b>Editing Configuration Profiles</b> for more details.	
OS	Displays the OS type which the profile supports.	
Author	Displays the name of the administrator who created the profile. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Created	Indicates the date and time at which the profile was created.	
Last Modified By	Displays the name of the last person who modified the profile. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Status	Indicates whether the profile has been successfully applied to devices. If the profile fails even in one device, it will show as 'Unsuccessful'. Clicking on this link will open the Device list screen, which displays the device details for which the profile was unsuccessful.	
#Devices	Indicates the number of devices for which the policy is assigned. Clicking the number will open the 'Devices associated with profile' screen, displaying the details of devices.	
Control Buttons		Enables the administrator to remove the profile.
	Create Android	Allows administrators to create a new Android profile. Refer to the section <b>Profiles for Android</b>

profile	<b>Devices'</b> for more details.
Create iOS profile	Allows administrators to create a new iOS profile. Refer to the section ' <b>Profiles for iOS Devices'</b> for more details.

### Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.



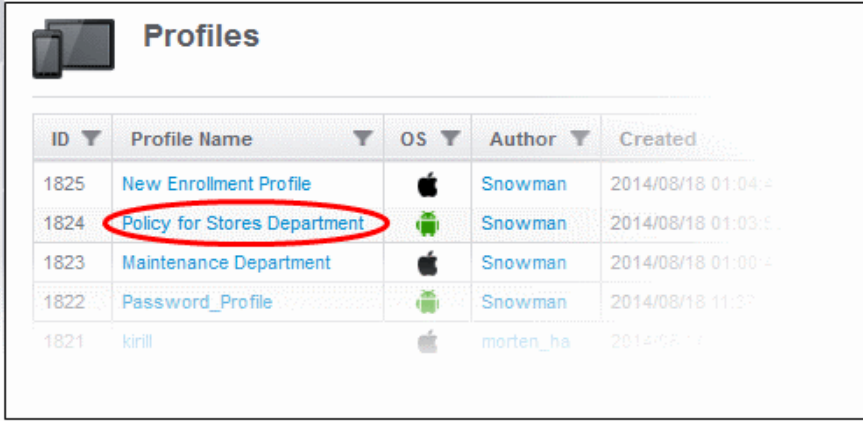
- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from the text field and click 'OK'.

## 4.3. Editing Configuration Profiles

A Profile that is already created can be edited according to the requirements of the organization.

### To edit a profile

- Click the 'Manage' tab from the left hand side navigation and choose 'Profiles' from the options.
- Click on the name of the profile that you want edit from the list.



ID	Profile Name	OS	Author	Created
1825	New Enrollment Profile	Apple	Snowman	2014/08/18 01:04
1824	Policy for Stores Department	Android	Snowman	2014/08/18 01:03
1823	Maintenance Department	Apple	Snowman	2014/08/18 01:00
1822	Password_Profile	Android	Snowman	2014/08/18 11:37
1821	kirill	Apple	morten_ha	2014/08/18

The Edit Profile screen for the selected profile will be displayed. The editing steps are similar to creating a new profile. Refer to the sections [Profiles for Android Devices](#) and [Profiles for iOS Devices](#) for more details.

## 4.4. Managing Default Profiles

Default profiles are very useful if you want to control the newly enrolled devices with certain policies before applying profiles according to the needs of the organization. You can create many default profiles, but make sure the settings in them do not conflict. If the settings in default profiles do conflict, then the Most Restricted policy will be applied. For example, if camera is enabled in a policy and disabled in another, then it will be disabled in the applied devices.

A default profile can be created from the 'Default profiles' screen, from the 'Profiles' interface or from the edit screen of existing Profiles screen. When you create a new profile from the 'Profiles' interface, you have the option to make the profile as also a default profile. When you create a default profile from the 'Default profile' screen, the 'Create profile' will open with the default checkbox preselected. Default profiles are automatically assigned to devices at the time of enrollment. Click the following links for more details:

- [Creating a default profile](#)
- [Viewing list of default profiles](#)
- [Assigning default profiles to devices](#)
- [Removing a default profile](#)

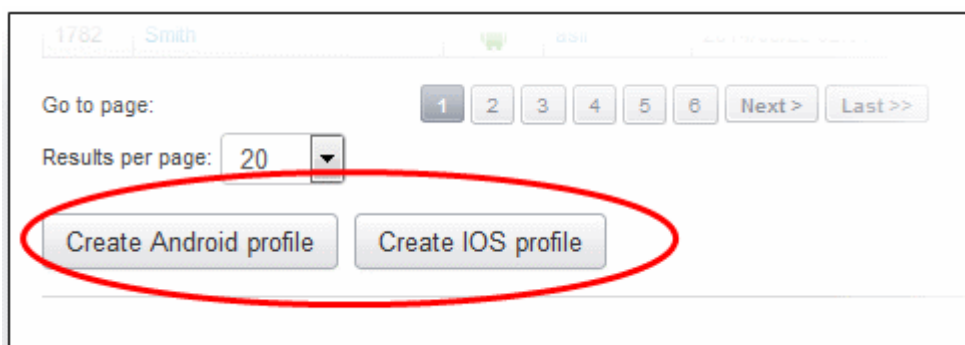
### Creating a default profile

A default profile can be created from the Create Profiles screen, from the Default profiles screen or in the edit screen of existing profiles. Click the following links to know more about creating default profiles.

- [Creating a default profile from the create profiles screen](#)
- [Creating a default profile from the default profile screen](#)
- [Creating a default profile from the edit screen of existing profiles](#)

### To create a default profile from the Create Profiles screen

- Click the Manage tab from the left side navigation
- Click Profiles
- Click on the type of profile that you want to create at the bottom of the screen



The new profile screen will be displayed.

- Select the 'Default profile' checkbox.

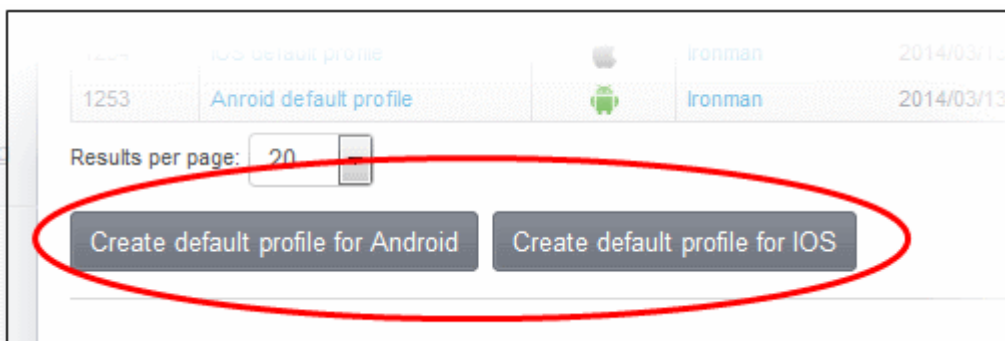
A screenshot of the 'New Android Profile' form. The breadcrumb trail is 'Home » Profiles » Create'. The title is 'New Android Profile' with a mobile device icon. The form has a 'Profile Name \*' field containing 'Default Android Profile'. Below it is a 'Default profile' checkbox, which is checked and circled in red. The 'Description' field contains 'Android profile for newly enrolled devices' and has a vertical scroll button. At the bottom, there is a 'Save' button and a note: 'Fields with \* are required.'

Create the profile as explained in the section **Creating Configuration Profiles**. The profile will be listed in the 'Default profiles' screen.

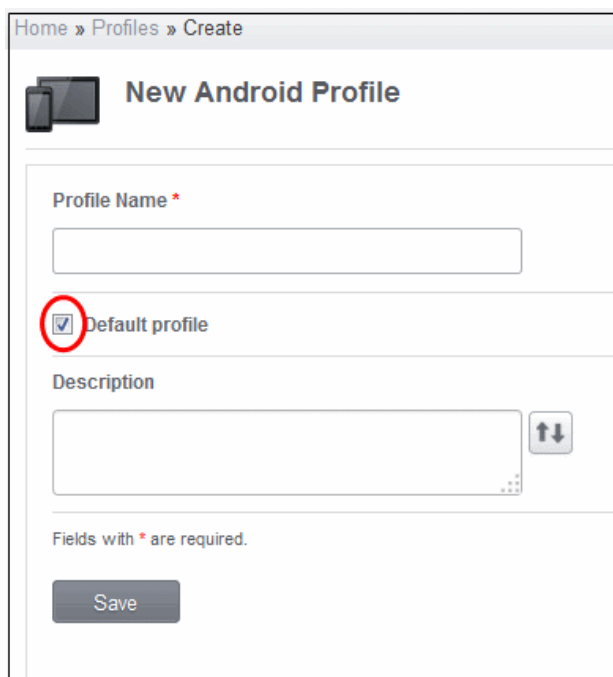
#### To create a default profile from the Default Profiles screen

- Click the Manage tab from the left side navigation
- Click Default Profiles
- Click on the type of default profile that you want to create at the bottom of the screen





The new profile screen will be displayed with the 'Default profile' checkbox preselected.



Create the profile as explained in the section **Creating Configuration Profiles**. The profile will be listed in the 'Default profiles' screen.

### To create a default profile from the Existing Profiles screen

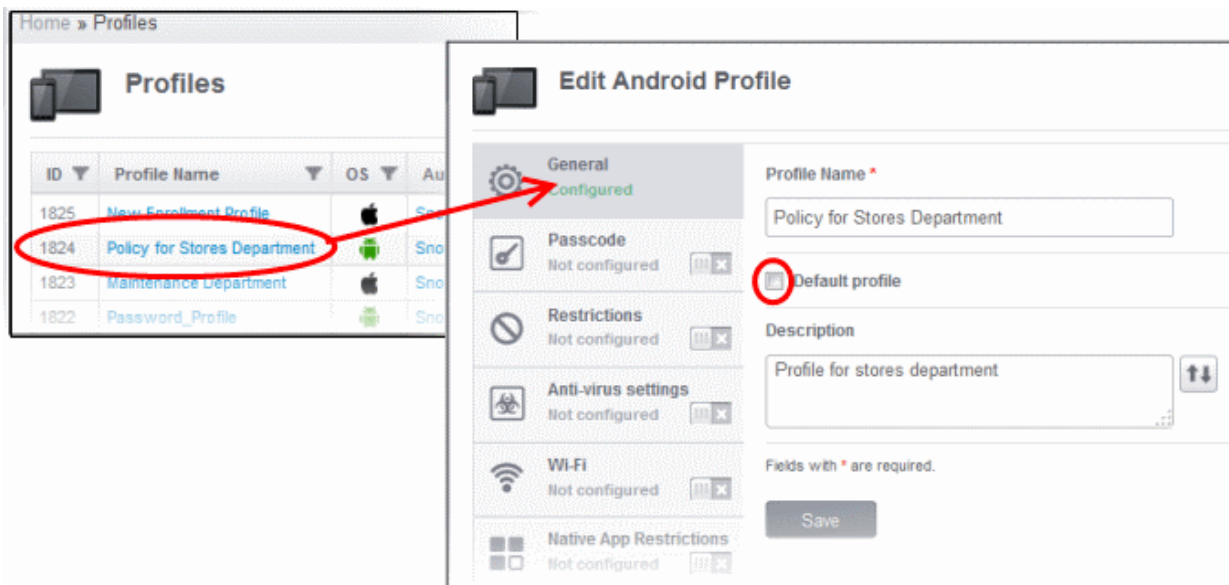
- Click the Manage tab from the left side navigation
- Click Profiles

The list of profiles will be displayed.

The screenshot shows the 'Profiles' screen with a table of existing profiles. The table has columns for ID, Profile Name, OS, Author, Created, Last Modified By, Status, and # devices.

ID	Profile Name	OS	Author	Created	Last Modified By	Status	# devices
1825	New Enrollment Profile	Apple	Snowman	2014/08/18 01:04:47 PM	Snowman	✓ Successful	0
1824	Policy for Stores Department	Android	Snowman	2014/08/18 01:03:53 PM	Snowman	✓ Successful	2
1823	Maintenance Department	Apple	Snowman	2014/08/18 01:00:41 PM	Snowman	✓ Successful	0
1822	Password_Profile	Android	Snowman	2014/08/18 11:37:13 AM	Snowman	✓ Successful	1

- Click on the name of a profile that you want to make it as a default profile.



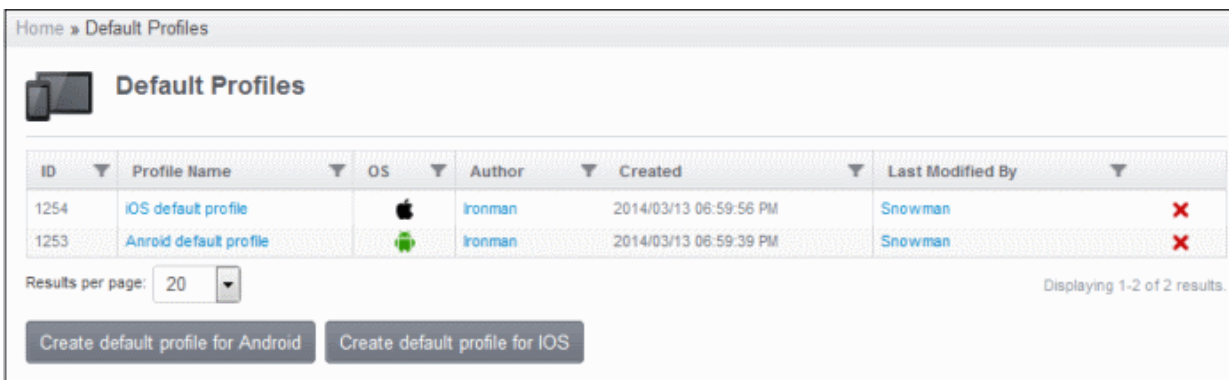
- Select the 'Default profile' checkbox and click the 'Save' button.

The profiles that were created will be listed in the 'Default profiles' screen.

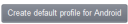
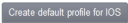
### To view the list of default profiles

- Click the Manage tab from the left side navigation
- Click Default profiles


The list of default profiles will be displayed in the screen.



Default Profiles - Column Descriptions	
Column Heading	Description
ID	The unique identity number assigned to the default profile.
Profile Name	Displays the name of the default profile. Clicking on the name will open the 'Edit Profiles' screen which displays the General details of the profile.
OS	Displays the OS type which the default profile supports.

Author	Displays the name of the person who created the profile. Clicking on the name link will display the full details of the user who created the default profile.	
Created	Indicates the date and time at which the default profile was created.	
Last Modified User	Displays the name of the last person who modified the profile. Clicking on the name link will display the full details of the user who modified the default profile.	
Control Buttons	<b>×</b>	Enables the administrator to remove the default profile.
		Enables the administrator to create a new default Android profile.
		Enables the administrator to create a new default iOS profile.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.

**Sorting**

---

Sort A to Z

Sort Z to A

**Advanced Filter**

---

Contains



---

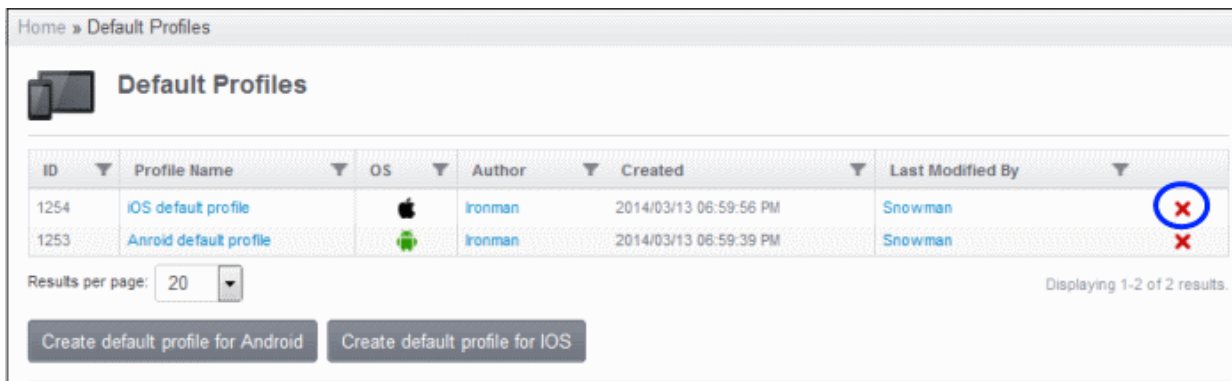
- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from the text field and click 'OK'.

## Assigning default profiles to devices

Devices that are enrolled for the first time will be automatically assigned the default profiles according to their operating system. These default profiles will be automatically overridden by regular profiles that are assigned to the devices by the administrator according to the organizational requirements. Please note the default profiles that were installed initially will become active again in the devices when the regular profiles are removed from them.

## Removing default profiles

You can remove the default profile from the 'Default profiles list' screen or from the 'Profiles list' screen. Click on the cross symbol at the far end in the row of the profile that you want to remove from the list.

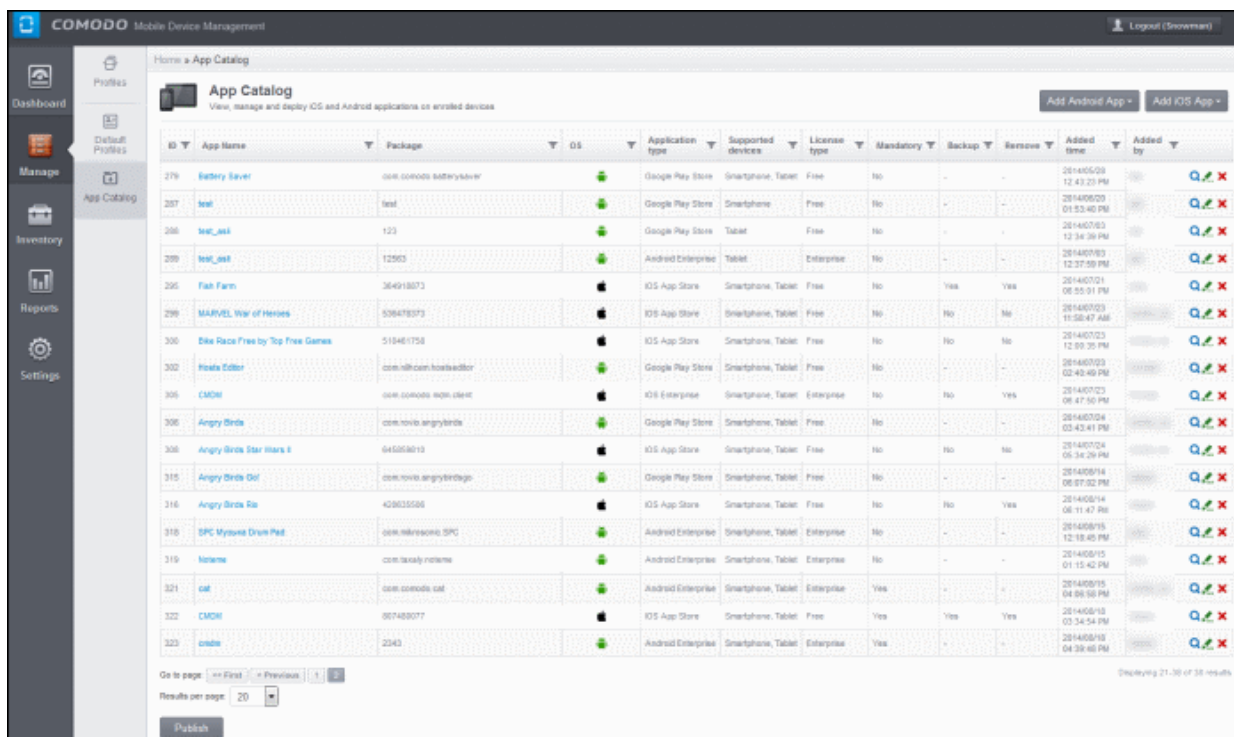


The default profile will be removed from the list and it will also be removed as a regular profile from the 'Profiles list' also. Please note that even if default profile(s) are removed from the list, the device(s) will still retain the configured settings from the profiles till a new profile(s) are assigned to them.

## 4.5. Managing Applications

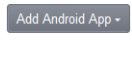
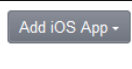




The App Repository interface in CMDM stores the path of Android apps and used to push them to enrolled devices. It can store apps from Google Play as well as third party apps. The interface allows to add, delete and update apps in CMDM.

To access the interface, click the 'Manage' tab from the left side navigation and then 'App Catalog'. The 'App Catalog' screen will be displayed.




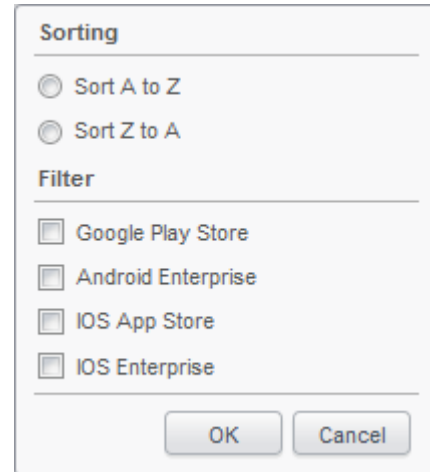
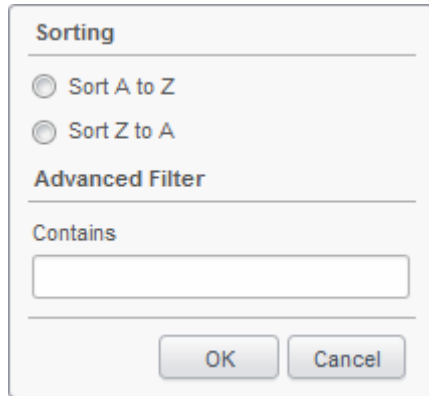
### Add Repository - Column Descriptions

Column Heading	Description
ID	The unique identity number assigned to the app.
App Name	Displays the name of the application. Clicking on the name of the app will open the respective

		application screen which displays the General details of the app.
Package		Displays the Bundle Identifier of the app.
OS		Displays the application OS type.
Application Type		Displays the type of app: <ul style="list-style-type: none"> <li>• Google Play Application</li> <li>• Android Enterprise Application</li> <li>• Application from iOS App Store</li> <li>• iOS Enterprise Application</li> </ul>
Supported Devices		Displays the type of devices that the app can work.
License Type		Indicates whether the app is a free, paid or enterprise version.
Mandatory		Indicates whether the app has been marked to be installed compulsorily on the devices. Refer to the section ' <b>Adding an app to the repository</b> ' for more details.
Backup		Indicates whether the app is allowed to be backed up to iTunes. This feature is available for iOS applications only. Refer to the section ' <b>Adding an app to the repository</b> ' for more details.
Remove		Indicates whether the app is allowed to be removed when MDM profile is removed. This feature is available for iOS applications only. Refer to the section ' <b>Adding an app to the repository</b> ' for more details.
Added Time		Indicates the date and time at which the app was added to repository.
Added By		Displays the name of the person who added the app to repository.
Control Buttons		Enables the administrator to add a new Google Play Store Application or Android Enterprise Application. Refer to the section ' <b>Adding an app to the repository</b> ' for more details.
		Enables the administrator to add a new iOS application from iOS Store or iOS Enterprise Application. Refer to the section ' <b>Adding an app to the repository</b> ' for more details.
		Apps added in this interface are synced automatically with the enrolled Android devices every 24 hours. In the Android and iOS devices, these apps can be viewed by tapping App Repository. To push the apps immediately to the devices after adding them here, click the 'Publish' button.
		Opens the details page of the app. Refer to the section ' <b>Viewing the details page</b> ' for more details.
		Opens the update page of the app. Refer to the section ' <b>Editing an app</b> ' for more details.
		Enables the administrator to delete the app from the list. Refer to the section ' <b>Deleting an app</b> ' for more details.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.



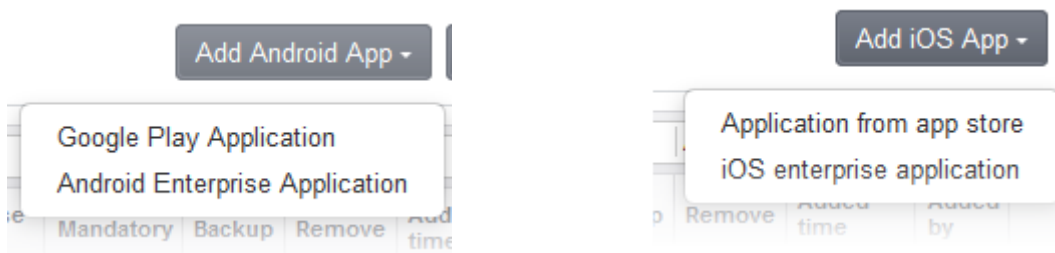
- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.

Click the following links for more details:



- [Adding an app to the repository](#)
- [Editing an app](#)
- [Deleting an app](#)
- [Viewing the details page](#)

## Adding an app to the app repository


- Click the 'Add Android App' or 'Add iOS App' button at the top right side of the screen and select the type of app that you want to add.



The Add Android/iOS application screen will open.

<h3> Add Google Play Application</h3> <p><b>Name</b></p> <input type="text"/> <hr/> <p><b>Version</b></p> <input type="text"/> <hr/> <p><b>Bundle ID</b> ⓘ</p> <input type="text"/> <hr/> <p><b>License type</b></p> <p><input type="radio"/> Free</p> <p><input type="radio"/> Paid</p> <hr/> <p><b>Category</b></p> <input type="text" value="Select Category"/> <hr/> <p><b>Supported devices</b></p> <input type="text" value="Select Supported Devices"/> <hr/> <p><b>Description</b></p> <input type="text"/> <hr/> <p><input type="checkbox"/> Mandatory app</p> <hr/> <p><b>Application logo</b></p> <input type="text" value="Browse..."/> No file selected. <hr/> <p><b>Application screenshots</b></p> <input type="text" value="Browse..."/> <hr/> <p><input type="button" value="Submit"/> <input type="button" value="Reset"/></p>	<h3> Add Enterprise Android Application</h3> <p><b>Name</b></p> <input type="text"/> <hr/> <p><b>Version</b></p> <input type="text"/> <hr/> <p><b>Bundle ID</b></p> <input type="text"/> <hr/> <p><b>Category</b></p> <input type="text" value="Select Category"/> <hr/> <p><b>Supported devices</b></p> <input type="text" value="Select Supported Devices"/> <hr/> <p><b>Description</b></p> <input type="text"/> <hr/> <p><b>Source file</b></p> <input type="text" value="Browse..."/> No file selected. <hr/> <p><b>Application logo</b></p> <input type="text" value="Browse..."/> No file selected. <hr/> <p><input type="checkbox"/> Mandatory app</p> <hr/> <p><input type="checkbox"/> Install&amp;Uninstall this application silently when possible</p> <hr/> <p><b>Application screenshots</b></p> <input type="text" value="Browse..."/> <hr/> <p><input type="button" value="Submit"/> <input type="button" value="Reset"/></p>
---	--



Add Android Application – Table of Parameters		
Form Element	Type	Description
Name	Text Field	Enter the name of the application.
Version	Text Field	Enter the version of the application.
Bundle ID	Text Field	<p>Enter the bundle identifier of the app. Usually this is must be in the reverse DNS format, for example, 'com.comodo.mobile.comodoantitheft'. In the Google Play store, the identifier is located between '=' and '&amp;' in the url. An example is shown below:</p> <p><b><a href="https://play.google.com/store/apps/details?id=com.comodo.pimsecure&amp;hl=en">https://play.google.com/store/apps/details?id=com.comodo.pimsecure&amp;hl=en</a></b></p> <p>The identifier, com.comodo.pimsecure, identifies this as Comodo Antivirus Free app.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p><b>IMPORTANT!!! CHANGE THE TEXT Steps to retrieve Bundle Identifier for Android Play Store Apps</b></p> <p>Follow the steps mentioned below to retrieve the bundle identifier for the Play Store Apps.</p> <ul style="list-style-type: none"> <li>- Go to Google Play Store (<a href="https://play.google.com/store">https://play.google.com/store</a>)</li> <li>- lets take Google Drive as the Play store App that you wanted to be added to the App repository</li> <li>- Click on the App or type the name of the App in the Google Play Search, so that the App opens</li> <li>- From the address bar, select the bundle identifier which is located between "=" and "&amp;" as displayed in the image below.</li> </ul>  <ul style="list-style-type: none"> <li>- Copy the Bundle Identifier and paste in the Bundle identifier field while adding the Play store App in App Repository.</li> </ul> </div> <p>Clicking the help icon beside the field displays how to retrieve the bundle identifier for the Play Store Apps.</p>
License Type	Radio Button	Select whether the app is free or a paid version. Note: This option is available in the 'Add Google Play application' form.
Category	Drop-down	Select the category to which the app belongs from the drop-down.
Supported devices	Drop-down	Select the type of device(s) that the app will support from the drop-down.
Description	Text Field	Enter the appropriate description for the app.
Mandatory app	Checkbox	If enabled, all enrolled devices will get alerts automatically to install the mandatory apps. Refer to the section <b>Installing Apps on Devices</b> for more details.
Install & Uninstall this application silently when possible	Checkbox	This can be enabled only when the 'Mandatory app' checkbox is selected. Enabling this option, the mandatory apps are installed silently without user interaction and uninstalling is done by tapping the Uninstall button in App Repository. This feature will work only for rooted and Samsung KNOX devices.
Application logo	Button	Upload application logo if required.
Application screenshots	Button	Upload application screenshots if required.
Source File	Browse button	Enables administrators to navigate and select the source file. Note: This option is available in the 'Add Android Enterprise application' form.
Submit	Button	The form is submitted and the path of the app is stored in the App Repository.
Reset	Button	Clears the form.

Add iOS Application – Table of Parameters		
Form Element	Type	Description
Name	Text Field	Enter the name of the application.
Version	Text Field	Enter the version of the application.
iTunes Store ID	Text Field	Enter the iTunes Store ID. This can be identified from the URL of the app. For example in the URL <a href="https://itunes.apple.com/us/app/CMDM/id807480077">https://itunes.apple.com/us/app/CMDM/id807480077</a> , the numbers after ID is the iTunes Store ID for this app.
iTunes Package name	Text Field	Enter the iTunes package name, for example com.comodo.cmdm.client
License Type	Radio Button	Select whether the app is free or a paid version. Note: This option is available in the 'Add iOS App Store Application' form.
Category	Drop-down	Select the category to which the app belongs from the drop-down.
Supported devices	Drop-down	Select the type of device(s) that the app will support from the drop-down.
Description	Text Field	Enter the appropriate description for the app.
Mandatory app	Checkbox	If enabled, the selected devices will get alerts to install the apps. Refer to the section <a href="#">Installing Apps on Devices</a> for more details.
Allow backup of the app data	Checkbox	If enabled, the user will be allowed to backup the application to iTunes
Remove app when MDM profile is removed	Checkbox	If enable, the app will be removed automatically when the MDM profile is removed.
Application logo	Button	Upload application logo if required.
Application screenshots	Button	Upload application screenshots if required.
Submit	Button	The form is submitted and the path of the app is stored in the App Repository.
Reset	Button	Clears the form.

Once the form is submitted, the app will be listed in the App Repository screen. Refer to the section [Installing Apps on Devices](#) to know how to install the selected apps in devices.

### Editing an app

- Click the update icon  at the far end in the row of app that you want to edit or update.

Or

- Click the view icon  and then the  button in the details page.

The 'Edit Application' screen will be displayed. This depends on the type of app you have selected, whether Play Store app, iOS App or Enterprise app to be updated.

### Edit iOS Application

**Name**

**Version**

**iTunes Store ID**

**iTunes Package name**

**License type**  
 Free  
 Paid

**Category**


**Supported devices**

**Description**

Mandatory app

Allow backup of the app data

Remove app when MDM profile is removed

**Application logo**  
  
 No file selected.

**Application screenshots**

### Edit Google Play Application

**Name**

**Version**

**Bundle ID**

**License type**  
 Free  
 Paid

**Category**

**Supported devices**

**Description**


Mandatory app

**Application logo**  
 No file selected.



**Application screenshots**

Edit or update the form. This is similar to adding an app and refer to the section **Adding an app** for more details.

## Deleting an app from the list

- Click the delete icon  at the far end in the row of app that you want to remove from the list.

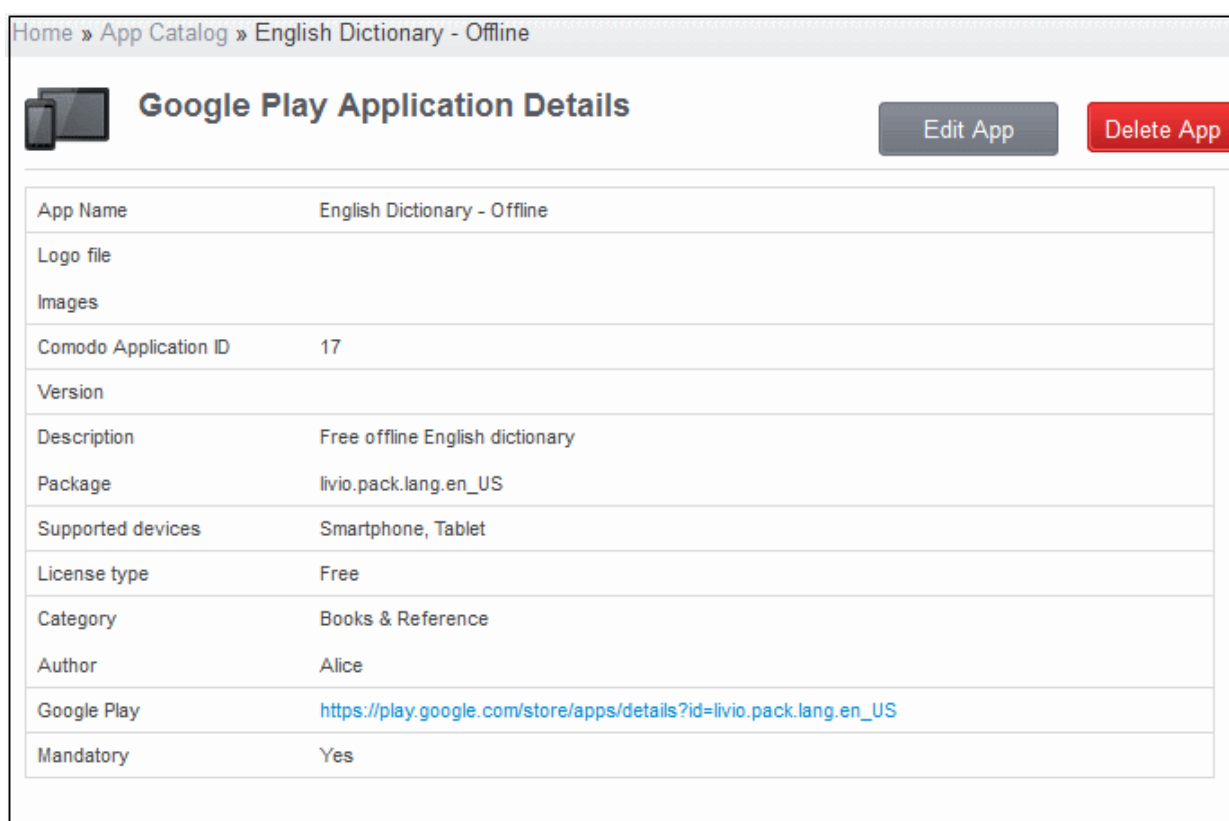
Or

- Click the view icon  and then the  button in the details page.
- Click 'OK' to confirm the deletion.

### Viewing the details page

- Click the view icon  at the far end in the row of app that you want to view the details.

The details of the app will be displayed in the page. The screen also allows to **edit** or **delete** the app from the list of repository.



Home » App Catalog » English Dictionary - Offline

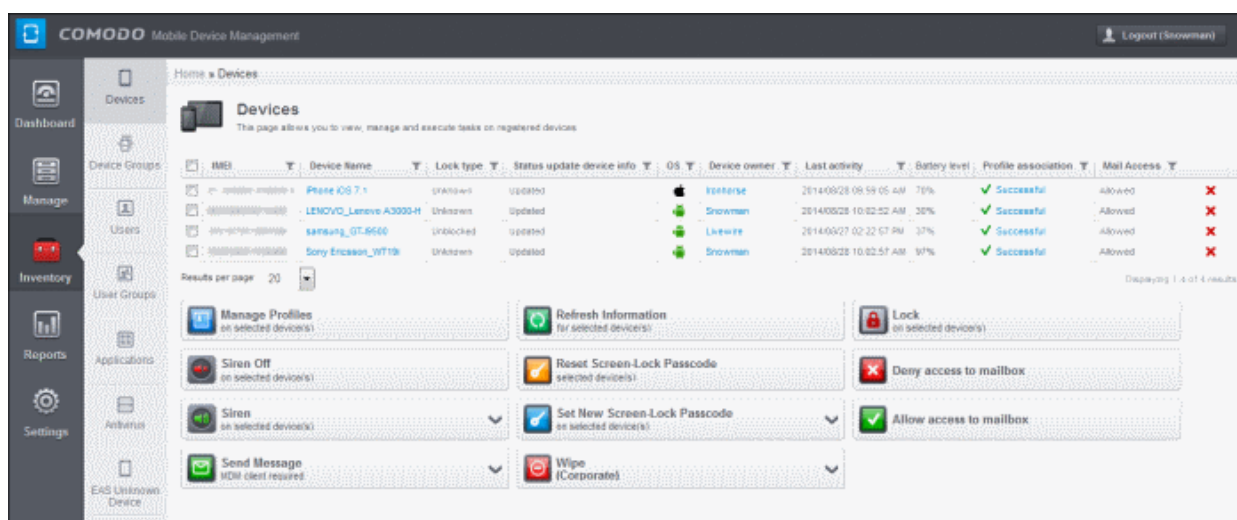
### Google Play Application Details

[Edit App](#) [Delete App](#)

App Name	English Dictionary - Offline
Logo file	
Images	
Comodo Application ID	17
Version	
Description	Free offline English dictionary
Package	livio.pack.lang.en_US
Supported devices	Smartphone, Tablet
License type	Free
Category	Books & Reference
Author	Alice
Google Play	<a href="https://play.google.com/store/apps/details?id=livio.pack.lang.en_US">https://play.google.com/store/apps/details?id=livio.pack.lang.en_US</a>
Mandatory	Yes

## 5. Managing Enrolled Devices and Users

The 'Inventory' tab enables the administrator to manage the users and enrolled devices and install applications on selected devices. The administrator can view the full information on any selected device with its current location on map and can take measures to prevent misuse of lost or stolen devices. The enrolled devices can be grouped according to the organization needs and appropriate configuration policies can be applied to each group. Also, the administrator can manage applications that can be allowed or to be blocked on the enrolled devices. The Antivirus feature in this tab allows administrators to run scan on devices as well as update AV database.



The following sections provide detailed explanations on managing the enrolled devices, users and the apps.

- **The Devices Interface**
  - **Managing an Individual Device**
  - **Viewing the location of the Device**
  - **Viewing the User Information**
  - **Removing a Device**
  - **Installing Apps on Devices**
  - **Generating Alarm on Selected Devices**
  - **Locking/Unlocking Selected devices**
  - **Configuring Access To Mailbox**
  - **Wiping Selected Devices**
  - **Assigning Configuration Policy to Selected Devices**
  - **Setting / Resetting Screen Lock Password for Selected Devices**
  - **Updating Device Information**
  - **Sending Text Messages to Devices**
- **Managing Device Groups**
  - **Creating Device Groups**
  - **Editing Device Groups**
  - **Assigning Configuration Policy to Groups**
- **Managing Users**
  - **Creating a New Users and Enrolling their Devices**
  - **Adding Devices for Management**
  - **Viewing the Details of a User**
  - **Updating the details of a User and Resetting Password**
  - **Assigning Configuration Profile to a User**
  - **Adding Devices for Enrollment**
  - **Removing a User**
- **Managing User Groups**
  - **Creating a New User Group**
  - **Editing a User Group**

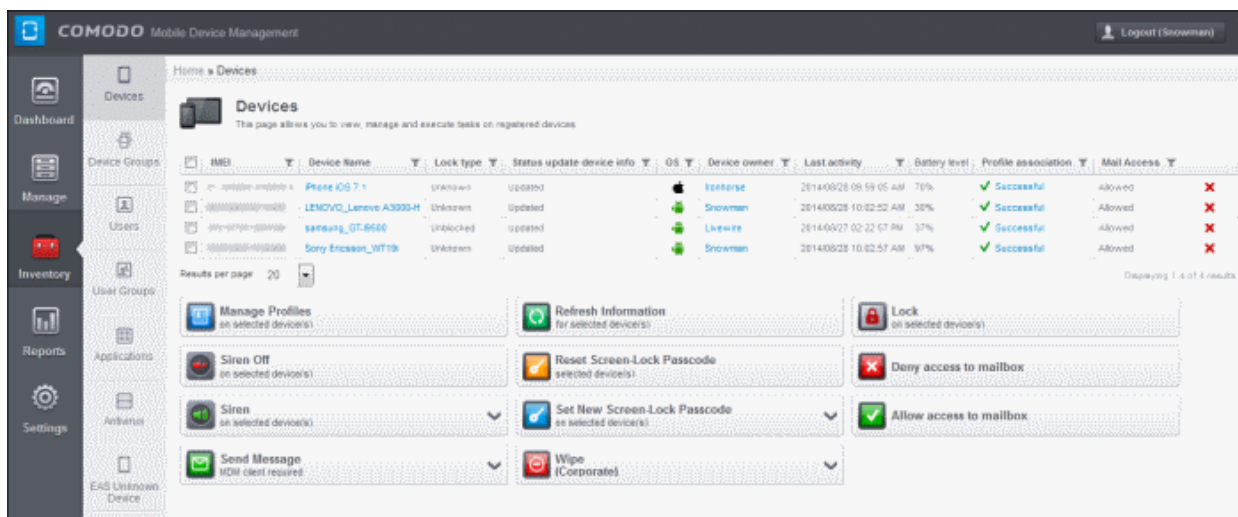
- [Assigning Configuration Profile to a User Group](#)
- [Removing a User Group](#)
- [Managing Applications on Enrolled Devices](#)
  - [Moving Selected Apps to Blacklist](#)
  - [Unblocking Blacklisted Apps](#)
- [Managing Antivirus and Running Scans on Enrolled Devices](#)
  - [Running On-demand Antivirus Scan](#)
  - [Updating AV Databases on Devices](#)

## 5.1. The Devices Interface

The 'Devices' interface displays a list of mobile devices that are enrolled to Mobile Device Manager, along with their details. The device periodically polls the CMDM server and updates the details displayed on this interface, hence accurately providing the latest values of remaining battery power and current CPU usage. The interface also allows the administrator to generate an alarm at selected devices, lock/unlock, wipe and powering off selected devices.

The individual devices can also be assigned with configuration profiles from the devices interface. The profile applied will be applied to the device in addition to the set of existing profiles applied to group, to which the device is a member of. In case the settings in a profile clashes with another profile, CMDM follows the 'Most Restricted' policy. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

To open the Devices interface, click the 'Inventory' tab from the left hand side navigation and choose 'Devices' from the options.




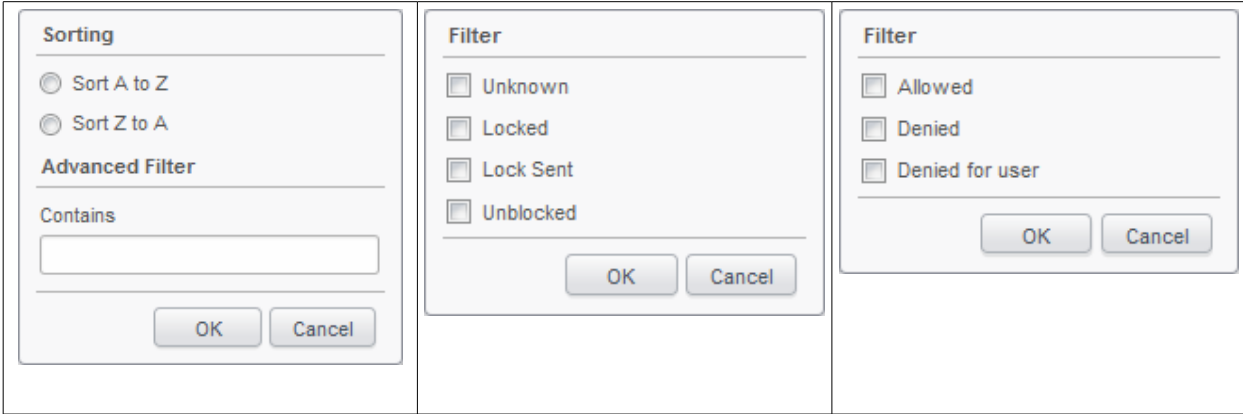
**Devices - Column Descriptions**

Column Heading	Description
IMEI	The International Mobile Equipment Identity (IMEI) number of the device.
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the View Device interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the section <a href="#">Managing an Individual Device</a> for more details.
Lock Type	Indicates whether the device is locked or unlocked. The administrator can lock or unlock a selected device by clicking the Lock/Unlock buttons below the table. Refer to the section <a href="#">Locking/Unlocking Selected devices</a> for more details.
Status Update Device Info	Indicates whether the device data is updated or not.

OS		Displays the Operating System of the device.
Device Owner		Indicates the owner/user of the device. Clicking the user name will open the View User interface, displaying the details of the user. Refer to the section <b>Viewing the Details of a User</b> for more details.
Last Activity		Indicates the date and time at which the device was last polled by CMDM.
Battery Level		Indicates the current remaining capacity of the battery in the device.
Profile Association		Indicates whether the profile(s) have been assigned successfully. Refer to the section <b>Assigning Configuration Profile to Selected Devices</b> for more details.
Mail Access		Indicates a user access status to mailbox including all devices associated with a current user. Refer to <b>Configuring Access To Mailbox</b> for more details.
Control Buttons	<b>X</b>	Enables the administrator to remove the device. Refer to <b>Removing a Device</b> for more details.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

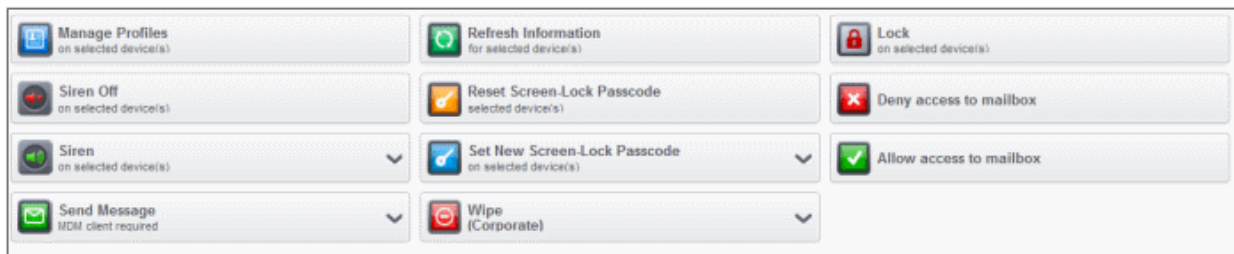
The buttons below the table enable the following:

- Sounding an alarm in the selected device(s) to identify its location, if it is lost or stolen or in case of emergency. Refer to the section **Generating Alarm on Selected Devices** for more details.
- Locking a lost or stolen device or unlocking a locked device. Refer to the section **Locking/Unlocking Selected Devices** for more details.
- Erase the device to prevent access to information stored on a lost or stolen device. Refer to the section **Wiping Selected Devices** for more details.
- Viewing/Assigning configuration profile on Selected Device. Refer to the section **Assigning Configuration Profile to Selected Device** for more details.
- Setting new passwords and resetting passwords for selected devices. Refer to the section **Setting / Resetting Screen**



**Lock Password for Selected Devices** for more details.

- Update device data. Refer to the section **Updating Device Information** for more details.
- Allow or deny the device(s) to access the corporate emails set up on a Exchange server. Refer to the section **Configuring Access To Mailbox** for more details.

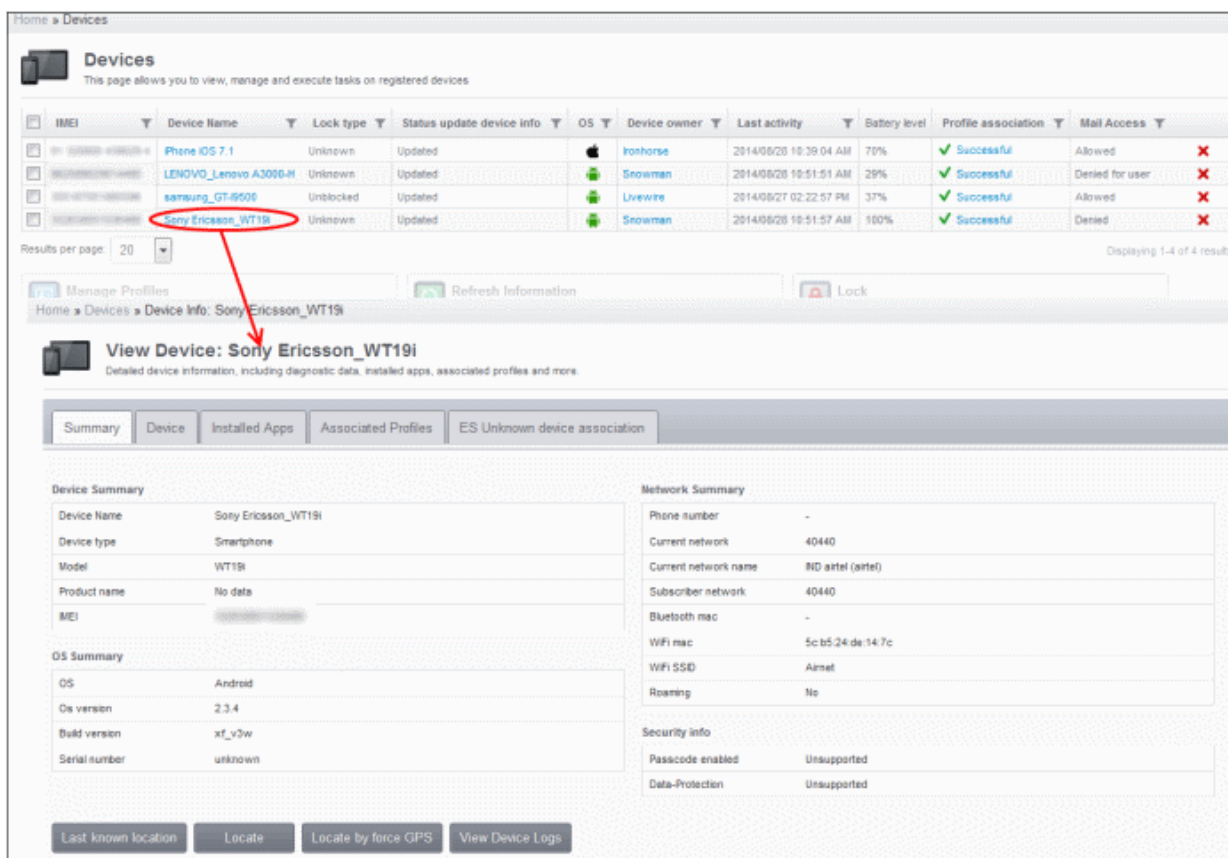


## 5.1.1. Managing an Individual Device

The administrator can view the complete hardware and software details of any enrolled device and manage the installed applications and configuration profiles in effect on the individual device. Also, the administrator can view the current location of the device on the map.

To view details of and manage an individual device

- Click the 'Inventory' tab from the left hand side and click 'Devices' from the options.
- Click on the name of the device



The 'View Device' pane will open, displaying the details of the selected device under four tabs:

- **Summary** - Displays the general details of the device including device information, OS details, Network details and security configuration. Refer to the section **Viewing Summary Information** for more details.
- **Device** - Displays the hardware and firmware information on the device, with current battery level and memory usage

status. Refer to the section **Viewing Hardware and Software Information** for more details.

- **Installed apps** - Displays a list of all the applications installed on the device and enables the administrator to manage the applications. Refer to **Managing Apps Installed on a Device** for more details.
- **Associated Profiles** - Enables the administrator to view the configuration profiles in effect on the device and to add new profiles or remove existing profiles. Refer to the section **Managing Profiles associated with the Device** for more details.
- **ES Unknown Device Association** - Enables the administrator to associate (to bind) unknown device from the quarantine list with devices from the CMDM list. Refer to the section **Associating EAS Unknown Devices** from the List for more details.

## 5.1.1.1. Viewing Summary Information

The 'Summary' tab in the 'View Device' interface displays the general information of the device.

### To view the device information summary

- Click the 'Inventory' tab from the left hand side and click 'Devices' from the options.
- Click on the name of the device to open the 'View Device' interface.
- By default the 'Device Summary' will be displayed, else click the 'Summary' tab.

Home » Devices » Device Info: Sony Ericsson\_WT19i

### View Device: Sony Ericsson\_WT19i

Detailed device information, including diagnostic data, installed apps, associated profiles and more.

Summary

Device

Installed Apps

Associated Profiles

ES Unknown device association

<p><b>Device Summary</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Device Name</td><td>Sony Ericsson_WT19i</td></tr> <tr><td>Device type</td><td>Smartphone</td></tr> <tr><td>Model</td><td>WT19i</td></tr> <tr><td>Product name</td><td>No data</td></tr> <tr><td>IMEI</td><td>352938051030400</td></tr> </table> <p><b>OS Summary</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>OS</td><td>Android</td></tr> <tr><td>Os version</td><td>2.3.4</td></tr> <tr><td>Build version</td><td>xf_v3w</td></tr> <tr><td>Serial number</td><td>unknown</td></tr> </table>	Device Name	Sony Ericsson_WT19i	Device type	Smartphone	Model	WT19i	Product name	No data	IMEI	352938051030400	OS	Android	Os version	2.3.4	Build version	xf_v3w	Serial number	unknown	<p><b>Network Summary</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Phone number</td><td>-</td></tr> <tr><td>Current network</td><td>40440</td></tr> <tr><td>Current network name</td><td>IND airtel (airtel)</td></tr> <tr><td>Subscriber network</td><td>40440</td></tr> <tr><td>Bluetooth mac</td><td>-</td></tr> <tr><td>WiFi mac</td><td>5c:b5:24:de:14:7c</td></tr> <tr><td>WiFi SSID</td><td>Airnet</td></tr> <tr><td>Roaming</td><td>No</td></tr> </table> <p><b>Security info</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Passcode enabled</td><td>Unsupported</td></tr> <tr><td>Data-Protection</td><td>Unsupported</td></tr> </table>	Phone number	-	Current network	40440	Current network name	IND airtel (airtel)	Subscriber network	40440	Bluetooth mac	-	WiFi mac	5c:b5:24:de:14:7c	WiFi SSID	Airnet	Roaming	No	Passcode enabled	Unsupported	Data-Protection	Unsupported
Device Name	Sony Ericsson_WT19i																																						
Device type	Smartphone																																						
Model	WT19i																																						
Product name	No data																																						
IMEI	352938051030400																																						
OS	Android																																						
Os version	2.3.4																																						
Build version	xf_v3w																																						
Serial number	unknown																																						
Phone number	-																																						
Current network	40440																																						
Current network name	IND airtel (airtel)																																						
Subscriber network	40440																																						
Bluetooth mac	-																																						
WiFi mac	5c:b5:24:de:14:7c																																						
WiFi SSID	Airnet																																						
Roaming	No																																						
Passcode enabled	Unsupported																																						
Data-Protection	Unsupported																																						

Last known location

Locate

Locate by force GPS

View Device Logs

- **Device Summary** - Provides device details such as brand, model and International Mobile Equipment Identification (IMEI) number.
- **OS Summary** - Provides details about the device Operating System (OS).
- **Network Summary** - Provides details about the mobile network to which the device is connected.
- **Security info** - Provides details about device storage encryption and passcode settings for screen unlock

- **Viewing Location of the device** - The buttons at the bottom of the summary pane enable administrators to view the location of the device on a map. Refer to **Viewing the Location of the Device** for more details.
  - Clicking 'Last known location' will show a map indicating the location of the device when it was last polled by CMDM
  - Clicking 'Locate' shows the current location of the device on a map
  - Clicking 'Locate by force GPS' acquires the current location of the device from the device GPS
- **Viewing Device Logs** – Opens the 'action log' for the device. Refer to the topic **Viewing Log of a Device** in **Viewing Event Logs from Individual Devices** section.


## 5.1.1.2. Viewing Hardware and Software Information

The 'Device' tab displays the hardware and OS information of the device, current memory state, current remaining battery level, whether the device is rooted or not. The pane also displays the details on the versions of MDM agent and its virus signature databases.

To view the Hardware and Software Information of a device

- Click the 'Inventory' tab from the left hand side and click 'Devices' from the options.
- Click on the name of the device to open the 'View Device' interface
- Click the 'Device' tab

Home » Devices » Device Info: Sony Ericsson\_WT19i



## View Device: Sony Ericsson\_WT19i

Detailed device information, including diagnostic data, installed apps, associated profiles and more.

Summary
Device
Installed Apps
Associated Profiles
ES Unknown device association

### Device information

Device Name	Sony Ericsson_WT19i
Device type	Smartphone
Last Connection	2014/08/26 03:08:43 PM
Registered	2014/08/26 09:30:41 AM
UUID	920ef09a6b77d335
Model	WT19i
Product name	No data
IMEI	352638051036466
OS	Android
OS Version	2.3.4
Build version	xf_v3w
Serial number	unknown
Phone number	-
Current network	40440
Current network name	IND airtel (airtel)
Subscriber network	40440
Bluetooth mac	-
WiFi mac	5c:b5:24:de:14:7c
WiFi SSID	Airnet
Roaming	-
Total RAM	335.3Mb
Available RAM	141.07Mb
Used RAM	194Mb
Available Internal Storage	0.22Gb
Total Internal Storage	0.41Gb
Available SD Storage	2.26Gb
Total SD Storage	3.67Gb
Cellular technology	GSM
Battery level	44%
Is rooted	-
Virus db version	103
Signs db version	38
Is unknown source enabled	Yes
Current application version	2.0.10.10
Byod type	<input type="text" value="Not specified"/>
Status update device info	Updated
Device Info Refreshed at	<span style="color: red;">Not set</span>

## 5.1.1.3. Managing Installed Applications

The 'Install Apps' tab in the 'View Device' interface displays a list of all the applications installed on the device and allows the administrator to block/unblock apps as required and uninstall selected apps that are found suspicious, not trust worthy, or junk apps from the device. The administrator can also identify the other enrolled devices, in which the same application has been installed, in order to replicate the corrective action, executed on the selected device.

### To manage installed apps

- Click the 'Inventory' tab from the left hand side and click 'Devices' from the options.
- Click on the name of the device to open the 'View Device' interface
- Click the 'Installed Apps' tab

Home » Devices » Device Info: Sony Ericsson\_WT19i

**View Device: Sony Ericsson\_WT19i**  
Detailed device information, including diagnostic data, installed apps, associated profiles and more.

Summary | Device | **Installed Apps** | Associated Profiles | ES Unknown device association

<input type="checkbox"/>	Name	Package	Version	Status
<input type="checkbox"/>	Xperia™ Hot Shots	com.sonyericsson.xhs	0.1.1	Allowed
<input type="checkbox"/>	Wisepilot	org.microemu.android.se.appello.lj.Lightpilot	0.1.1	Allowed
<input type="checkbox"/>	UEFA.com	com.afj.seucom.view	1.0.0	Allowed
<input type="checkbox"/>	Music Unlimited	com.sony.snei.mu.phone	1.0.2	Allowed
<input type="checkbox"/>	McAfee Security	com.wsandroid.suite	1.0.0.7	Allowed
<input type="checkbox"/>	WhatsApp	com.whatsapp	2.6.4184	Allowed
<input type="checkbox"/>	Google Settings	com.google.android.gms	5.0.89 (1307510-032)	Allowed

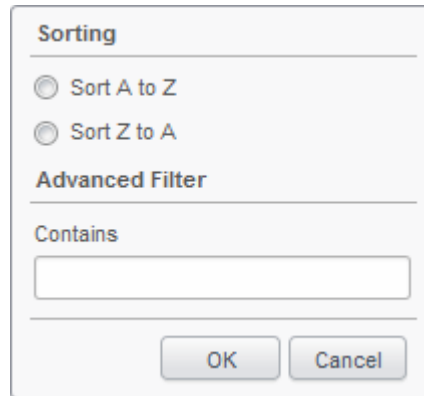
Results per page: 20 | Displaying 1-7 of 7 results.

Block | Unblock | Uninstall | Update Application List

Installed Apps - Column Descriptions	
Column Heading	Description
Name	The name of the application. Clicking the name of the application will open the ' <b>Devices</b> ' interface, listing only the devices in which the same application is installed. This makes it easier for the administrator to identify the devices and block or uninstall a suspicious, malicious or junk application from other devices too.
Package	Indicates the source of the application, i.e downloaded android/.iOS package, from which the application has been installed.
Version	Indicates the version of the application.
Status	Indicates whether the application is allowed to run, blocked, blacklisted or in the process of uninstalling.

### Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.



**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

Contains

OK Cancel

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from the text field and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

#### Blocking, unblocking, uninstalling and updating application list

- To block unwanted app(s) from execution in the device, select the app(s) and click 'Block'.
- To release blocked apps(s) and allow them to run, select the blocked app(s) and click 'Unblock'.
- To uninstall malicious or junk app(s) from the device, select the app(s) and click 'Uninstall'. A notification will be sent to the device and the app will be immediately blocked. Upon user seeing the notification and clicking 'Uninstall' from the notification, the app will be uninstalled from the device.
- Normally the list of apps in a device is updated to CMDM every 24 hrs. To update the list immediately, click the 'Update Application List' button.

#### 5.1.1.4. Managing Profiles Associated with the Device

The 'Associated Profiles' tab lists the configuration profiles in effect on the device. It also allows the administrator to add or remove profiles. If multiple profiles are associated with the device, the most restrictive policy will be applied. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

For more details on profiles and groups of profiles, refer to the chapter [Managing Configuration Profiles and Apps](#).

##### To manage applied configuration profiles

- Click the 'Inventory' tab from the left hand side and choose 'Devices'
- Click on the name of the device to open the 'View Device' interface
- Click the 'Associated Profiles' tab

The list of profiles associated with the devices will be displayed.

Home » Devices » Device Info: Sony Ericsson\_WT19i

**View Device: Sony Ericsson\_WT19i**  
Detailed device information, including diagnostic data, installed apps, associated profiles and more.

Summary | Device | Installed Apps | **Associated Profiles** | ES Unknown device association


ID ▼	Profile Name ▼	Created	Source associated	Applied	Status ▼	Error message
1253	<a href="#">Anroid default profile</a>	2014/03/13 06:59:39 PM	Default	2014/08/26 03:16:51 PM	✓ Successful	

Results per page:  ▼ Displaying 1-1 of 1 result

[Add / remove profiles](#)

Associated Profiles - Column Descriptions	
Column Heading	Description
ID	The Unique ID number assigned to the profile.
Profile Name	The name assigned to the profile by the administrator. Clicking the name of a profile will open the 'Edit Profile' interface. Refer to the section <b>Editing Configuration Profiles</b> for more details.
Created	Indicates the date and time at which the profile was created.
Source Associated	Indicates the status of the device to which the profile is associated. For example, if the device is in a group and profile is applied, then it will display as Device Groups. It will show as Device if a profile is applied to it individually. Clicking on Device Groups link will display the Manage Profiles for Android Device Group(s) screen with the profile applied to the group preselected. Clicking on the Device link will display the 'Association profiles on devices' screen with the profiles applied to the device preselected.
Applied	Indicates the date and time at which the profile was applied.
Status	Indicates whether the profile has been successfully applied to devices.
Error message	If a profile associated is not successful, the error message is displayed.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.

**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

Contains

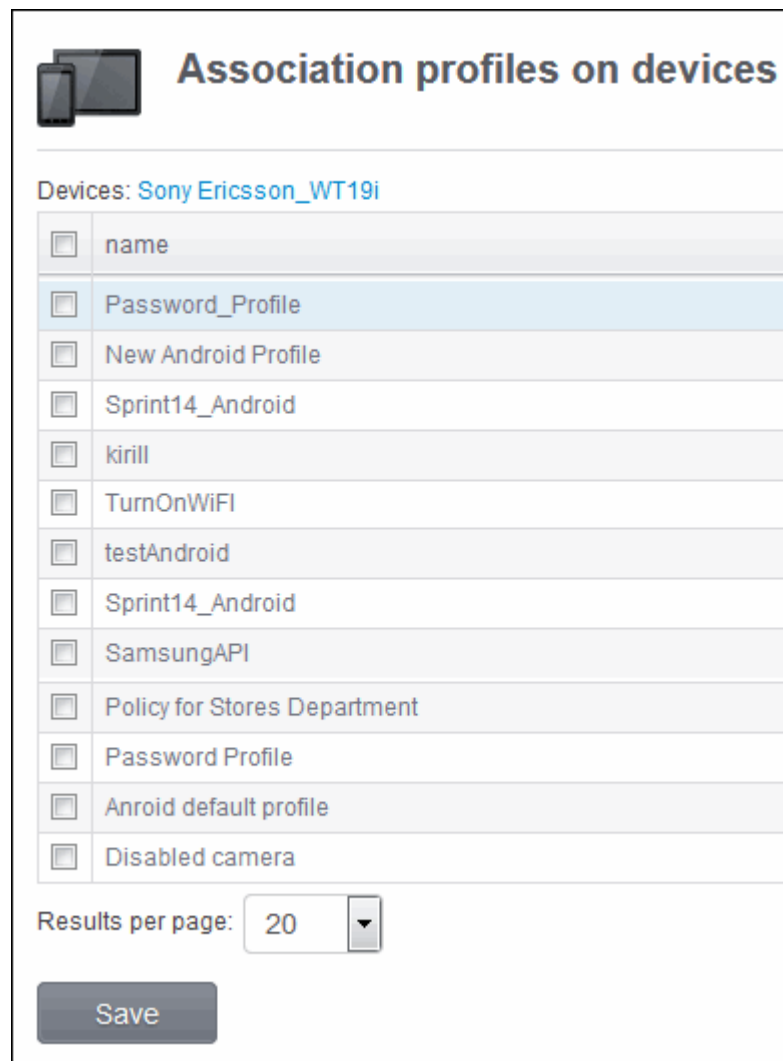


- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from the text field and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

### To add/remove profiles

- Click the 'Add/Remove profile' button.

The 'Associate profiles on devices' interface will open displaying the configuration profiles that is associated with the device preselected.



**Association profiles on devices**

Devices: [Sony Ericsson\\_WT19i](#)

<input type="checkbox"/>	name
<input checked="" type="checkbox"/>	Password_Profile
<input type="checkbox"/>	New Android Profile
<input type="checkbox"/>	Sprint14_Android
<input type="checkbox"/>	kirill
<input type="checkbox"/>	TurnOnWiFi
<input type="checkbox"/>	testAndroid
<input type="checkbox"/>	Sprint14_Android
<input type="checkbox"/>	SamsungAPI
<input type="checkbox"/>	Policy for Stores Department
<input type="checkbox"/>	Password Profile
<input type="checkbox"/>	Anroid default profile
<input type="checkbox"/>	Disabled camera

Results per page: 20 ▼

**Save**

- To add profile to the device, select the checkbox beside it in the screen.
- To remove a profile from the device, deselect the checkbox beside it.
- Click 'Save' for your changes to take effect.

### 5.1.1.5. Associating EAS Unknown Devices

The 'EAS Unknown Device to associate' tab allows the administrator to view a list of all unknown not associated devices from the quarantine list and to bind with current device from the CMDM portal. It also allows the administrator to disassociate the device.

## To associate unknown device

- Click the 'Inventory' tab from the left hand side and click 'Devices' from the options.
- Click on the name of the device to open the 'View Device' interface
- Click the 'EAS Unknown device to association' tab
- Click the 'Associate to device'. The list of unknown devices will be displayed.

EAS Unknown devices - Column Descriptions	
Column Heading	Description
ID	The Unique ID number assigned to the device.
IMEI	The International Mobile Equipment Identity (IMEI) number of the device.
Phone number	Displays the phone number of the user.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device.
Model	Indicates the model number of the device.
Os	Displays the OS type which the device supports.

The EAS Associated Device summary will be displayed.

Home » Eas Unknown Device to associate

### List of EAS Unknown Devices to associate

	Id	Imei	Phone number	Name	Model	Os
⊙	android1407242843874			Nexus 7	Nexus 7	Android 4.4.4

Results per page:  Displaying 1-1 of 1 result.

- Click the 'Disassociate' button to disconnect the device.

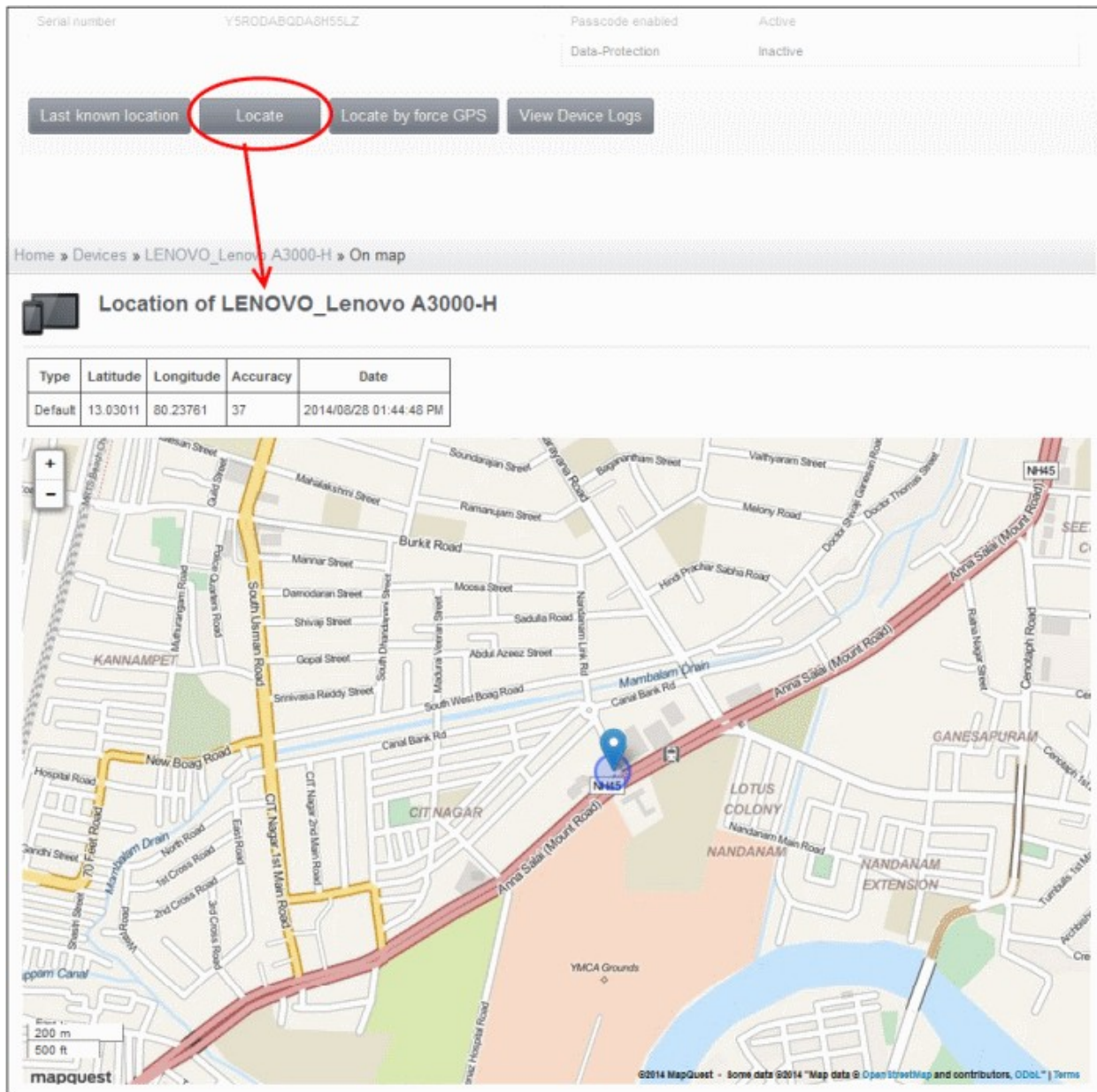
## 5.1.2. Viewing the Location of the Device

The CMDM console has the ability to show the real time location of the device on a map. This is useful if the phone is lost or stolen or if the administrator wishes to track the device for other reasons.

### To locate the device

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Click on the device name to open the 'View Device' panel of the device
- To view the current location of the device, click the 'Locate' button at the bottom of the Summary screen.

The location will be displayed on map.



- If the device is currently not connected to Internet or switched-off, you can view the location of the device during its last polling time with CMDM server by clicking the 'Last known location' button under the 'Summary' tab.
- Click 'Locate by force GPS' button to view the location using device GPS.

### 5.1.3. Viewing the User Information

The administrator can view and update user details such as email address and phone number from the 'Devices' interface.

#### To view the user information of a device

- Select 'Inventory' from the left hand menu then click 'Devices'.
- The users of each device are listed in the 'Device owner' column. Click a user's name to open the 'View User' pane
- Click the 'Update' link at top-left to modify user details. For more details on this area, see **Viewing the details of the User** section.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association
	LENOVO_Lenovo A3000-H	Unknown	Updated		Snowman	2014/08/28 01:55:37 PM	22%	✓ Successful
	samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful
	Sony Ericsson_WT19i	Unknown	Updated		Snowman	2014/08/28 01:54:47 PM	92%	✓ Successful

Results per page: 20

Manage Profiles on selected device(s)

Home » Users » User Info: Snowman

### View User: Snowman

Update

ID	2968
Username	Snowman
Email	fiatlena@gmail.com
Phone number	
User created	2014/08/14 12:37:42 PM
Last login	2014/08/28 01:24:01 PM
Token Expire	2014/08/30 12:53:02 PM
Token Left	3
Token status	Active
# of Devices	2
Change password time	2014/08/14 01:26:16 PM

Lock on selected device(s)

Clicking the 'Update' link at the top left enables the administrator to update the user details. Refer to the section [Viewing the details of the User](#) for more details.

### 5.1.4. Removing a Device

CMDM allows administrators to remove enrolled devices from the interface and when the process is complete, these devices can no longer be managed using the CMDM interface. When a device is de-enrolled, the CMDM agent and configuration profiles will be automatically wiped. The CMDM app can also be removed by users when the devices are de-enrolled.

#### To remove a device from the interface

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device(s) that you want to de-enroll.
- Click the **✘** button at the far end of the row.

Home » Devices

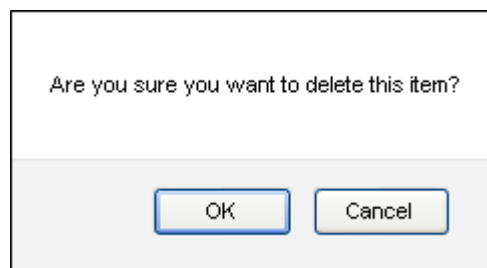
**Devices**  
This page allows you to view, manage and execute tasks on registered devices

<input type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input type="checkbox"/>	862589025614495	LENOVO_Lenovo A3000-H	Unknown	Updated		Snowman	2014/08/28 02:08:14 PM	21%	✓ Successful	Denied for user
<input type="checkbox"/>	355167051885596	samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed
<input type="checkbox"/>	352638051036466	Sony Ericsson_WT19i	Unknown	Updated		Snowman	2014/08/28 02:09:10 PM	91%	✓ Successful	Denied

Results per page: 20 Displaying 1-3 of 3 results

on selected device(s)
 for selected device(s)
 on selected device(s)

- Click 'OK' to confirm removal of the device in the confirmation dialog.



The device will be removed from the list.

#### To remove CMDM app on Android devices

- Navigate to Settings > Applications > Manage Applications
- Tap 'Comodo MDM'
- Tap the 'Uninstall' button.

The CMDM app will be removed from the device.

#### To remove CMDM profile on iOS devices

- Navigate to Settings > General
- Tap on Comodo Profiles (certificate and Comodo MDM)
- Tap the 'Remove' button.

The CMDM profile will be removed from the device.

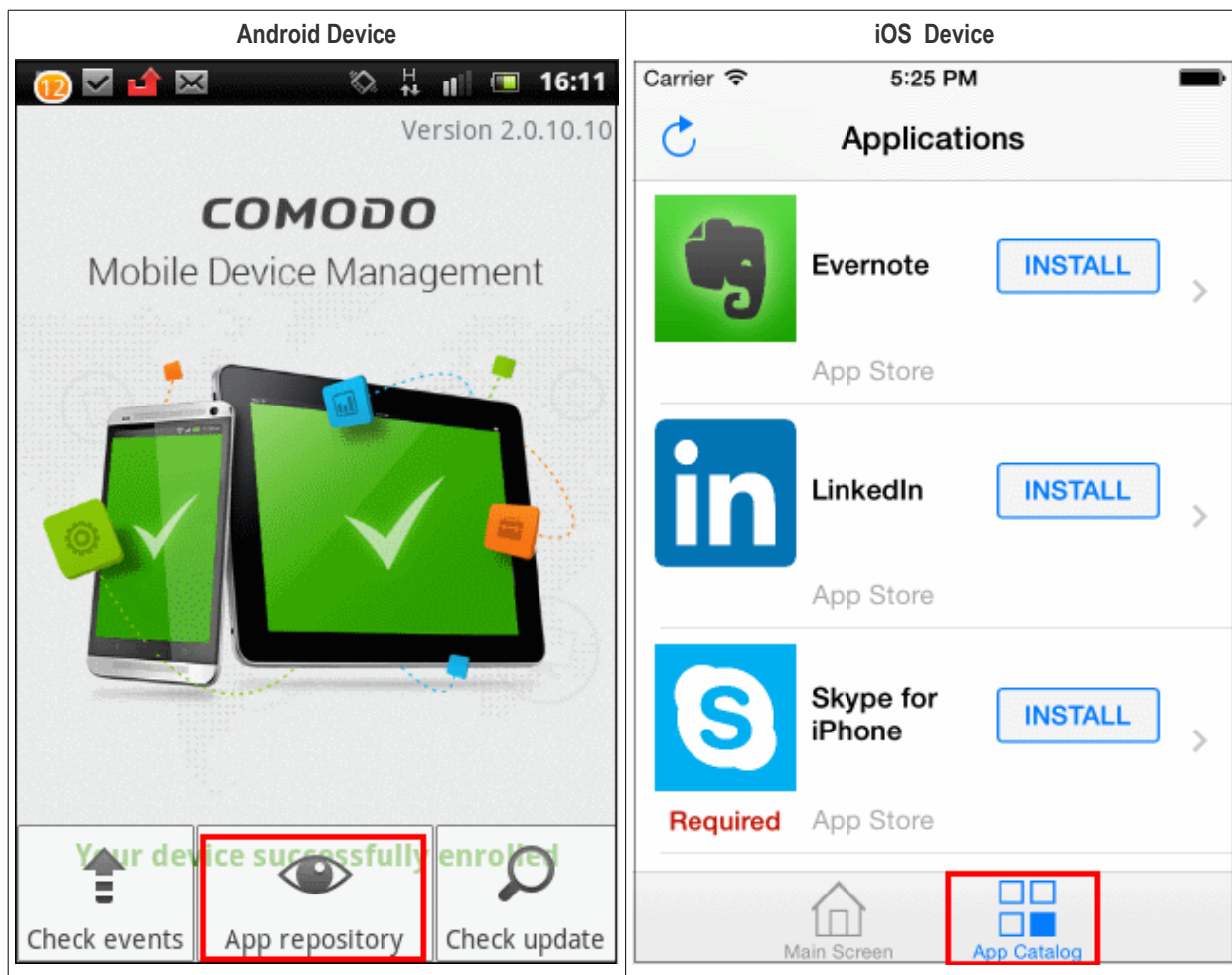
**Note:** If the user has already removed the CMDM app from the device, then after deletion from the Devices screen it will be listed in 'Removal Confirmation' list. The device can be enrolled again only after this device is removed from the Removal Confirmation list. Refer to the section '[Viewing and Managing Removed Devices](#)' for more details.

## 5.1.5. Installing Apps on Devices

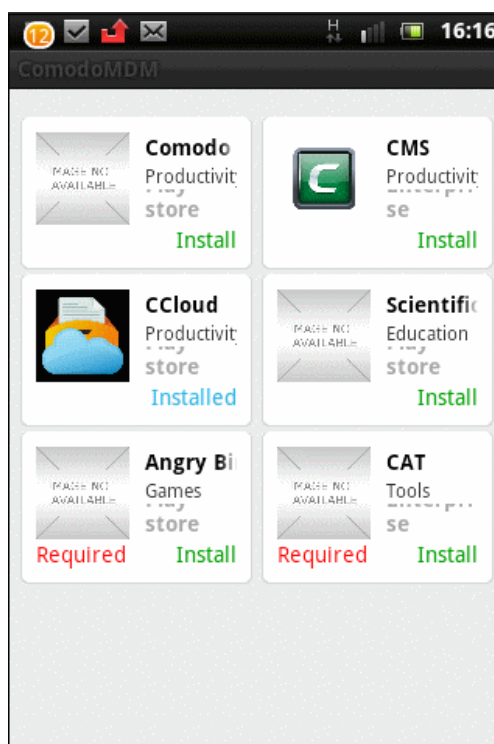
CMDM allows administrators to push applications to all devices. Applications that the administrator intends to roll-out to user devices can be added to the CMDM **App Catalog**. The sync between the CMDM server and the devices takes place every 24



hours or immediately when the 'Publish' button is pressed. For more details on uploading application packages to the CMDM Apps Catalog, refer to the section **Managing Applications**. The apps can be viewed on any device by tapping the 'App Repository' and 'App Catalog' tab on Android and iOS devices respectively in the CMDM app.



The App Repository screen in the device displays the synced apps.



The screen displays a list of all catalog apps that have been installed and any required apps that are awaiting installation. The 'Required' red text indicates the apps are marked as mandatory in **App Catalog**.

- Tap 'Install' to download and install the apps.

If apps have been marked as mandatory in **App Catalog**, then the users will be alerted frequently until they are installed. If the user uninstalls a mandatory app, again alerts will be sent to the device to install them again.



- Tap 'Install required apps' and install the mandatory apps.

### 5.1.6. Generating Alarm on a Device

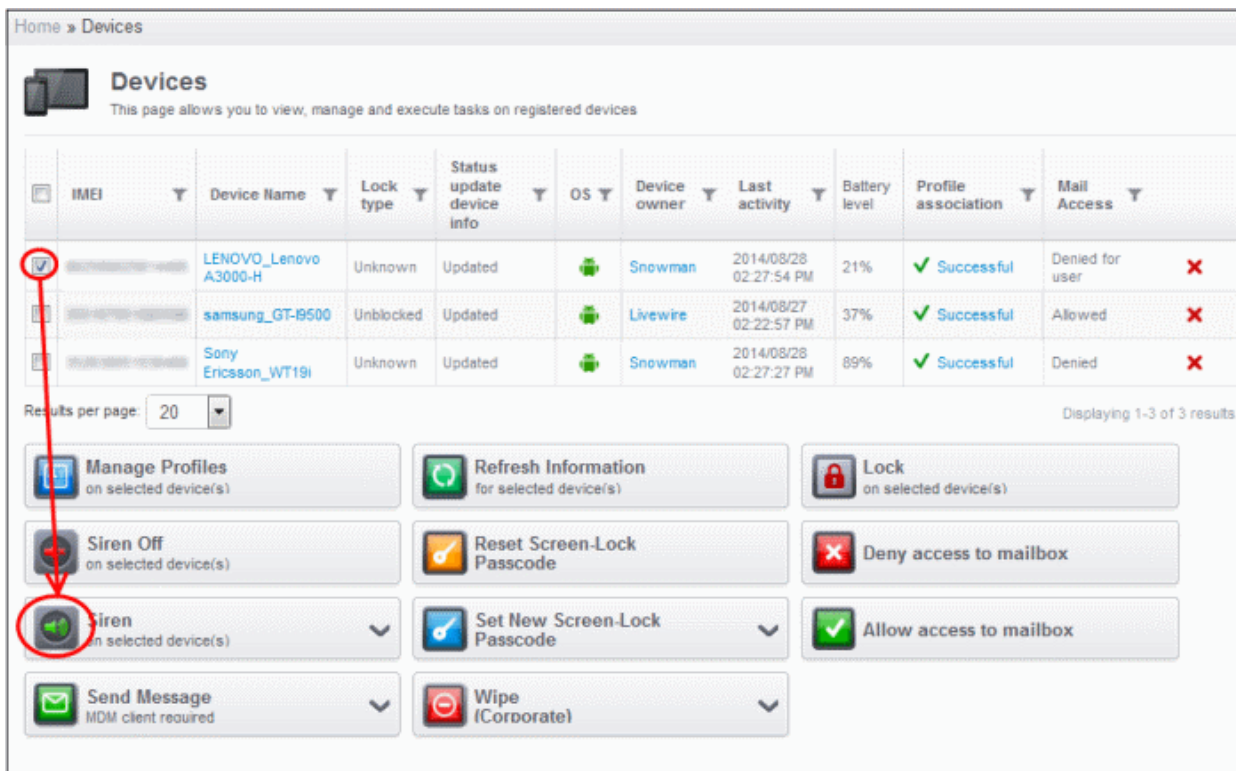
If a device is mislaid, lost or stolen, upon user's request, the administrator can make the device to sound an alarm to precisely locate the device. The device will start to emit a loud alarm at full volume, even if it is in silent mode. Once the device is located or identified, the administrator can stop the alarm from the 'Devices' interface of the CMDM management console. The alarm can also be used to grab the attention of user.

**Note:** This feature is available only for Android devices.

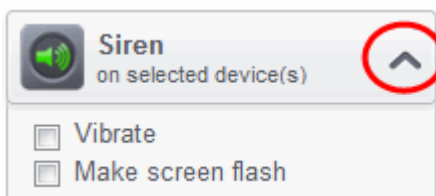
#### To generate an alarm

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device on which the alarm has to be generated.





- Select the alarm options by clicking the expand button:



- Vibrate - The device will vibrate along with the siren
- Make screen flash - The device screen will flash intermittently along with the siren
- Click the 'Siren On' button.

The device will start emitting the loud alarm.

### To stop the siren

- Select the device from the 'Devices' interface.
- Click the 'Siren Off' button.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input checked="" type="checkbox"/>	[REDACTED]	LENOVO_Lenovo A3000-H	Unknown	Updated	Android	Snowman	2014/08/28 02:27:54 PM	21%	✓ Successful	Denied for user
<input type="checkbox"/>	[REDACTED]	samsung_GT-B9500	Unblocked	Updated	Android	Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed
<input type="checkbox"/>	[REDACTED]	Sony Ericsson_WT19i	Unknown	Updated	Symbian	Snowman	2014/08/28 02:27:27 PM	89%	✓ Successful	Denied

Results per page: 20 Displaying 1-3 of 3 results.

**Manage Profiles**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Lock**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren**  
on selected device(s)

**Set New Screen-Lock Passcode**

**Allow access to mailbox**

**Send Message**  
MDM client required

**Wipe**  
(Corporate)

## 5.1.7. Locking/Unlocking Selected Devices

Administrators can remotely send screen lock command from the CMDM devices screen to prevent mislaid devices from being accessed by unauthorized persons or to generally block access to a device. After the lock command is sent, the selected device(s) are automatically locked. The user can unlock by entering the screen lock password in the device.

**Note:** This feature is available only for Android devices.

### To remotely lock a device

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device to be locked.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input checked="" type="checkbox"/>	Sony Ericsson_WT19i	Unlocked	Updated	Android	Snowman	2014/09/01 11:22:09 AM	64%	✓ Successful	Allowed
<input type="checkbox"/>	LENOVO_Lenovo A3000-H	Unlocked	Updated	Android	Snowman	2014/09/01 11:21:13 AM	29%	✓ Successful	Allowed
<input type="checkbox"/>	samsung_GT-I9500	Unlocked	Updated	Android	LiveWire	2014/08/27 02:22:57 PM	37%	✓ Successful	Denied

Results per page: 20 Displaying 1-3 of 3 results

**Manage Profiles**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Siren**  
on selected device(s)

**Send Message**  
MDM client required

**Refresh Information**  
for selected device(s)

**Reset Screen-Lock Passcode**

**Set New Screen-Lock Passcode**

**Wipe (Corporate)**

**Lock**  
on selected device(s)

**Deny access to mailbox**

**Allow access to mailbox**

- Click the 'Lock' button.

The lock command will be sent. The lock status of the device will be indicated as 'Lock Sent' under the 'Lock Type' column. The device will be locked and the user can unlock the device by entering the screen lock password.

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input type="checkbox"/>	Sony Ericsson_WT19i	Lock Sent	Updated	Android	Snowman	2014/09/01 11:28:25 AM	63%	✓ Successful	Allowed
<input type="checkbox"/>	LENOVO_Lenovo A3000-H	Unlocked	Updated	Android	Snowman	2014/09/01 11:28:02 AM	31%	✓ Successful	Allowed
<input type="checkbox"/>	samsung_GT-I9500	Unlocked	Updated	Android	LiveWire	2014/08/27 02:22:57 PM	37%	✓ Successful	Denied

Once the command is successfully executed on the device, it will be locked and the Lock Type will change to 'Locked'.

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input type="checkbox"/>	Sony Ericsson_WT19i	Locked	Updated	Android	Snowman	2014/09/01 11:32:52 AM	63%	✓ Successful	Allowed
<input type="checkbox"/>	LENOVO_Lenovo A3000-H	Unlocked	Updated	Android	Snowman	2014/09/01 11:32:22 AM	32%	✓ Successful	Allowed
<input type="checkbox"/>	samsung_GT-I9500	Unlocked	Updated	Android	LiveWire	2014/08/27 02:22:57 PM	37%	✓ Successful	Denied

Results per page: 20

### To unlock a locked device

The device can be unlocked by the user by entering the screen lock password that has been set for the device. After the device is unlocked, the status of the device under the 'Lock type' will display as 'Unlocked'.

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
	Sony Ericsson_WT19i	Unblocked	Updating		Snowman	2014/09/01 11:38:29 AM	62%	✓ Successful	Allowed
	LENOVO_Lenovo A3000-H	Unblocked	Updated		Snowman	2014/09/01 11:37:53 AM	34%	✓ Successful	Allowed
	samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed

Results per page: 20

## 5.1.8. Configuring Access to Mailbox

The buttons 'Allow access to mailbox' and 'Deny access to mailbox' will be available in the Devices screen only after **installing the Exchange Service** and successful communication with CMDM server. Administrators can be choose to allow or deny the users access to mailbox via their devices from this interface.

### To deny access to mailbox

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device that is to be allowed access to mailbox.

Home » Devices

**Devices**  
This page allows you to view, manage and execute tasks on registered devices

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
862589025614485	LENOVO_Lenovo A3000-H	Unknown	Updated		Snowman	2014/08/28 11:40:55 PM	1%	✓ Successful	Denied for user
862589025614485	samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed

Results per page: 20

Displaying 1-2 of 2 results.

Manage Profiles on selected device(s)
  Refresh Information for selected device(s)
  Lock on selected device(s)

Siren Off on selected device(s)
  Reset Screen-Lock Passcode
  Deny access to mailbox

Siren on selected device(s)
  Set New Screen-Lock Passcode
  Allow access to mailbox

Send Message MDM client required
  Wipe (Corporate) selected device(s)

- Click the 'Deny access to mailbox' button.

The deny command will be sent. Once the command is successfully executed on the device, it will be denied access to the mailbox. The status will display as 'Denied for device' under the Mail Access' column.

**Note:** All devices associated with definite user will be blocked if IMEI of a device is not identified.

### To allow access to mailbox

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device that is denied access to mailbox.

The status of the device will be indicated as 'Denied' under the 'Mail Access' column.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input checked="" type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input checked="" type="checkbox"/>		samsung_GT-I9500	Unblocked	Updated	Android	Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Denied

Results per page: 20 Displaying 1-1 of 1 result.

**Manage Profiles**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Lock**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren**  
on selected device(s)

**Set New Screen-Lock Passcode**

**Allow access to mailbox**

**Send Message**  
MDM client required

**Wipe (Corporate)**  
selected device(s)

- Click the 'Allow access to mailbox' button.

Access to mailbox for user is granted.

- The allow command will be sent and after successful execution, the device can access mailbox.

## 5.1.9. Wiping Selected Devices

Information security is of utmost importance in any organization. Confidential corporate documents and sensitive information like usernames and passwords of users, contacts, stored messages, browser bookmarks pictures and so on stored in the device/SD card, are prone to be misused by criminal from a stolen or lost device. In order to prevent the leak of such information, the administrator can remotely erase the contents from a lost device from the 'Devices' interface.

### To erase the contents stored in a device

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device to be wiped.



Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access	
<input checked="" type="checkbox"/>	355-96-736-0101140	LENOVO_Lenovo A3000-H	Lock Sent	Updated	Android	Snowman	2014/08/28 11:40:55 PM	1%	✓ Successful	Denied for user	✗
<input type="checkbox"/>	355-96-736-0101140	samsung_GT-I9500	Unblocked	Updated	Android	Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed	✗

Results per page: 20 Displaying 1-2 of 2 results.

**Manage Profiles**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Lock**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren**  
on selected device(s)

**Set New Screen-Lock Passcode**

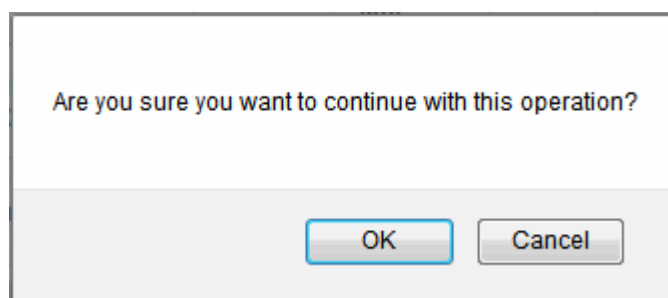
**Allow access to mailbox**

**Send Message**  
MDM client required

**Wipe (Corporate)**  
selected device(s)

Corporate Wipe (removes your...)

- Select the content to be erased
  - To remove only CMDM agent and configuration profiles, select 'Corporate Wipe' from the drop-down below the Wipe button
  - To erase all the data from the device and the SD card, select 'Full Wipe' from the drop-down. The device will be returned to default factory settings after the wipe operation.
- Click the 'Wipe' button. A confirmation dialog will be displayed.



- Click OK in the confirmation dialog.

The content in the device will be erased as chosen from the drop-down.

## 5.1.10. Assigning Configuration Profile to Selected Devices

The 'Devices' interface allows the administrator to view the current configuration profiles applied to selected devices and to apply new configuration profiles to them. The profile applied from this interface adds up to the device along with the existing profiles applied to the group to which the device is a member of. In case the settings in a profile clashes with another profile, CMDM follows the 'Most Restricted' policy. For example, if a profile allows the use of camera and another restricts its use, the device will not be able to use the camera as per the 'Most Restricted' policy.

For more details on profiles and groups of profiles, refer to the chapter [Managing Configuration Profiles and Apps](#).

**Tip:** You can view and manage the profiles for a single device from the 'View Device' panel. Refer to the section **Managing Profiles Associated with the Device** for more details.

### To view the profiles applied to a device

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device and click the 'Manage Profiles' button.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
[icon]	Sony Ericsson_WT19i	Unblocked	Updated	[android]	Snowman	2014/09/01 12:05:00 PM	57%	✓ Successful	Allowed
[icon]	LENOVO_Lenovo A3000-H	Unblocked	Updated	[android]	Snowman	2014/09/01 12:05:07 PM	41%	✓ Successful	Allowed
[icon]	samsung_GT-I9500	Unblocked	Updated	[android]	LiveWire	2014/08/27 02:22:57 PM	37%	✓ Successful	Denied

Results per page: 20 | Displaying 1-3 of 3 results.

**Manage Profiles** on selected device(s)

**Refresh Information** for selected device(s)

**Lock** on selected device(s)

**Siren Off** on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren** on selected device(s)

**Set New Screen-Lock Passcode**

**Allow access to mailbox**

**Send Message** MDM client required

**Wipe (Corporate)**

The 'Associate profiles on devices' interface will open with the profiles applied to the device preselected.



## Association profiles on devices

---

Devices: [samsung\\_GT-I9500](#)

<input type="checkbox"/>	name
<input type="checkbox"/>	Password_Profile
<input type="checkbox"/>	New Android Profile
<input type="checkbox"/>	kirill
<input type="checkbox"/>	test_A
<input type="checkbox"/>	Smith
<input type="checkbox"/>	TurnOnWiFi
<input type="checkbox"/>	testAndroid
<input type="checkbox"/>	Sprint14_Android
<input type="checkbox"/>	SamsungAPI
<input type="checkbox"/>	Profile_password_test_complexity
<input type="checkbox"/>	Policy for Stores Department
<input type="checkbox"/>	Anroid default profile
<input checked="" type="checkbox"/>	CoolWiFi
<input type="checkbox"/>	Password Profile
<input type="checkbox"/>	Disabled camera

Results per page:  ▼

**Note:** If the device is in a group, the profiles applied to the group will not be indicated here. To view the the profiles applied to a device group refer to the section [Assigning Configuration Profiles to Groups](#).

- To add a profile to the device, select the checkbox beside it.
- To remove a profile from the device, deselect the checkbox beside it.
- Click 'Save' for your changes to take effect.

### 5.1.11. Setting / Resetting Screen Lock Password for Selected Devices

The Devices interface allows administrators to set or reset screen lock password remotely for enrolled devices.

**Note:** This feature is available only for Android devices.

#### To set a new screen lock password

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device.

- Click on the Expand button in 'Set New Screen-Lock Passcode'.
- Enter the screen-lock password in the Password field. Select the 'Show password' checkbox to view the password.
- Click on the key button.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input checked="" type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access	
<input checked="" type="checkbox"/>		samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed	✗

Results per page: 20 Displaying 1-1 of 1 result.

**Manage Profiles**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Siren**  
on selected device(s)

**Send Message**  
MDM client required

**Wipe (Corporate)**  
selected device(s)

**Refresh Information**  
for selected device(s)

**Reset Screen-Lock Passcode**

**Set New Screen-Lock Passcode**

Password:   Show password

**Lock**  
on selected device(s)

**Deny access to mailbox**

**Allow access to mailbox**

The command will be sent to the device and next time this new password should be entered on the device to unlock the screen.

**Note:** If a Passcode profile has been configured for the selected device, make sure to enter the new password that complies with the profile.

### To reset a screen lock password

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device.
- Click the 'Reset Screen-Lock Passcode' button.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input checked="" type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input checked="" type="checkbox"/>	XXXXXXXXXXXX	samsung_GT-I9500	Unlocked	Updated	Android	Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed

Results per page: 20 Displaying 1-1 of 1 result.

**Manage Profiles**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Lock**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren**  
on selected device(s)

**Set New Screen-Lock Passcode**

**Allow access to mailbox**

**Send Message**  
MDM client required

**Wipe (Corporate)**  
selected device(s)

The command will be sent to the device and the current screen lock password will be cleared. A message also will be sent to the device regarding the screen lock password change. If a Password profile is configured in the device, the user will be required to enter a new password that complies with the profile.

### 5.1.12. Updating Device Information

CMDM agent in the enrolled devices sends full information such as memory status, name of the device, IMEI number, roaming state, MAC address of bluetooth, MAC address of WiFi and so on to the server at periods configured in the settings interface. If required, these information can be fetched on real time by clicking the 'Refresh Information' button in the interface.







#### To update device information

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device.
- Click the 'Refresh Information' button.


Home » Devices


## Devices


This page allows you to view, manage and execute tasks on registered devices


IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access	
	LENOVO_Lenovo A3000-H	Lock Sent	Updated		Snowman	2014/08/28 11:40:55 PM	1%	✓ Successful	Denied for user	
	samsung_GT-I9500	Unblocked	Updated		Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed	


Results per page: 20 Displaying 1-2 of 2 results.


 **Manage Profiles**  
on selected device(s)


 **Refresh Information**  
for selected device(s)


 **Lock**  
on selected device(s)


 **Siren Off**  
on selected device(s)


 **Reset Screen-Lock Passcode**


 **Deny access to mailbox**

 **Siren**  
on selected device(s)

 **Set New Screen-Lock Passcode**

 **Allow access to mailbox**

 **Send Message**  
MDM client required

 **Wipe (Corporate)**  
selected device(s)

The Status Update Device info column will display as 'Updating' for the selected device(s) and when done, it will display as 'Updated'.

### 5.1.13. Sending Text Message to Devices

CMDM allows administrators to send text messages to enrolled devices. This will come in handy if the user should be sent some important notifications such as to change screen lock password that complies with the passcode profile and so on.

#### To send text message to devices

- Click the 'Inventory' tab from the left hand side and choose 'Devices' from the options.
- Select the device(s).
- Click on the Expand button in 'Send Message'.
- Enter the text message in the Description field.
- Click on the Send Message button.

Home » Devices

## Devices

This page allows you to view, manage and execute tasks on registered devices

<input checked="" type="checkbox"/>	IMEI	Device Name	Lock type	Status update device info	OS	Device owner	Last activity	Battery level	Profile association	Mail Access
<input checked="" type="checkbox"/>	3520140827022257	samsung_GT-I9500	Unlocked	Updated	Android	Livewire	2014/08/27 02:22:57 PM	37%	✓ Successful	Allowed

Results per page: 20 Displaying 1-1 of 1 result.

**Manage Profiles**  
on selected device(s)

**Refresh Information**  
for selected device(s)

**Lock**  
on selected device(s)

**Siren Off**  
on selected device(s)

**Reset Screen-Lock Passcode**

**Deny access to mailbox**

**Siren**  
on selected device(s)

**Set New Screen-Lock Passcode**

**Allow access to mailbox**

**Send Message**  
MDM client required

Description  
Hi Livewire. The battery is low. Please recharge immediately

**Wipe (Corporate)**  
selected device(s)

The message will be sent to the selected device(s) for the users' attention.

## 5.2. Managing Device Groups

Comodo MDM allows the administrator to create logical device groups of Android and iOS devices for convenient management of large number of mobile devices. For example, the devices can be grouped as per the structure of the organization and/or depending on types of devices. The administrator may create groups of devices called 'Sales Department', 'Accounts Department', 'Android Tablets', '7" iPads', 'Android Smart Phones', 'iPhones' or 'All Managed Mobile Devices'.

Once created, the administrator can manage all devices belonging to that group together. Dedicated configuration profiles can be created for each group as per their requirements and the allowable user privileges and applied appropriately to the device groups. For more details on creating and managing configuration profiles, refer to the chapter **Managing Configuration Profiles and Apps**.

The 'Devices Groups' interface displays the list of device groups and allows the administrator to create new groups, import devices into groups and assign configuration profiles to the groups as required.

To open the 'Devices Groups' interface, click the 'Inventory' tab from the left hand side navigation and choose 'Device Groups' from the options.

Home » Group devices

## Device Groups


ID	Group name	Os type	Creator user	Time creation	Last modified user	
169	Marketing Department	Android	Yuliya	2014/08/20 03:27:10 PM	Yuliya	✗
23	Test Group	Android	John_Smith	2014/01/21 02:11:18 PM	asli	✗
18	Sales Dept	Android	Smith	2013/11/07 10:22:14 AM	asli	✗
17	Marketing iOS Devices	iOS	Smith	2013/11/07 10:21:21 AM	asli	✗
3	Smith	iOS	asli	2014/06/25 02:01:47 AM	asli	✗

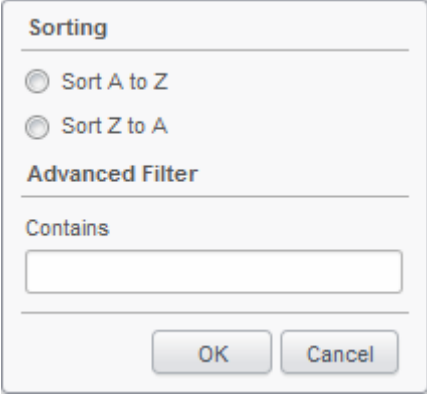
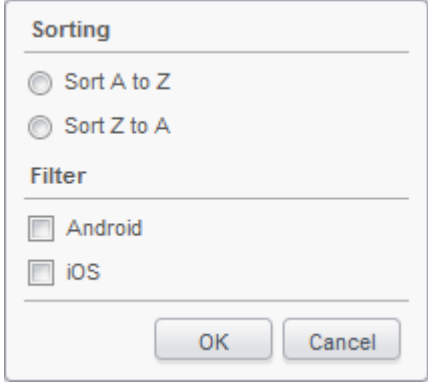
Results per page: 20 Displaying 1-5 of 5 results.

Group devices - Column Descriptions		
Column Heading	Description	
ID	The Identity (ID) Number assigned to the device group.	
Group name	The name assigned to the device group by the administrator. Clicking the name of a group will open the 'Device group' interface that displays the list of devices included in the group with check box selected beside them and allows you to add or remove devices to/from the group. Refer to the section <b>Editing Device Groups</b> for more details.	
OS type	The Operating System (OS) of the devices in the group.	
Created user	Indicates the administrator that has created the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Time Creation	Indicates the date and time at which the group was created.	
Last Modified User	Indicates the administrator that has recently edited the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Control Buttons	✗	Enables the administrator to remove the group.
	Manage Profiles	Allows administrators to manage configuration profiles to selected device groups.
	Create Android device group	Allows administrators to create a new Android device group.
	Create iOS device group	Allows administrators to create a new iOS device group.



## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

From the Devices Groups interface, the administrator can:

- Create Device Groups**
- Edit Device Groups**
- Assign Configuration Policy to Groups**
- Remove a Device Group**

### 5.2.1. Creating Device Groups


Administrators can create device groups as required and import mobile devices into it. The grouping of devices enables pushing selected configuration profiles to all the devices pertaining to a group at-once. The groups are to be created separately for different OS types. Refer to the sections below for detailed explanations on creating the groups:

- Creating an Android Device Group**
- Creating an iOS Device Group**

#### To create an Android device group

- Open the 'Devices Groups' interface by clicking the 'Inventory' tab from the left hand side and choosing 'Device Groups'
- Click the 'Create Android devices group' button at the bottom of the interface. The 'Create/Edit Device Group' interface will open.

Home » Group devices » Create



## Create/Edit Device Group

Select devices to become members of a device group.

Group name \*

<input type="checkbox"/>	name
<input type="checkbox"/>	LENOVO_Lenovo A850
<input type="checkbox"/>	LGE_LG-P715
<input type="checkbox"/>	samsung_GT-I9500
<input type="checkbox"/>	ZTE_Blade S
<input type="checkbox"/>	HUAWEI_HUAWEI-U8850

Results per page: 20 ▼

The devices available for importing are displayed.

- Enter the name to be assigned to the group in the 'Group name' text box.
- Select the devices to be imported into the group from the list.
- Click 'Save'. The new group will be created.

Group of devices successfully created. ✕

The new group will be listed in the 'Group devices' interface. Appropriate configuration profiles can now be applied to the new group. Refer to [Assigning Configuration Policy to Groups](#) for more details.

### To create an iOS device group

- Open the 'Devices Groups' interface by clicking the 'Inventory' tab from the left hand side and choosing 'Device Groups'
- Click the 'Create iOS devices group' button at the bottom of the interface. The 'Create/Edit Device Group' interface will open.

Home » Group devices » Create

## Create/Edit Device Group

Select devices to become members of a device group.

Group name \*

<input type="checkbox"/>	name
<input type="checkbox"/>	New iOS device
<input type="checkbox"/>	iPhone5 - Blue
<input type="checkbox"/>	iPhone 4s(Comodo)

Results per page: 20 ▼

Save

The devices available for importing into the group are displayed.

- Enter the name to be assigned to the group in the 'Group name' text box.
- Select the devices to be imported into the group from the list.
- Click 'Save'. The new group will be created.

Group of devices successfully created. ✕

The new group will be listed in the 'Group devices list' interface. Appropriate configuration profiles can now be applied to the new group. Refer to [Assigning Configuration Policy to Groups](#) for more details.

## 5.2.2. Editing Device Groups

The administrator can view the member devices of a group and can add or remove devices, from the 'Device Groups' interface.

### To view and edit device groups

- Open the 'Device Groups' interface by clicking the 'Inventory' tab from the left hand side and choosing 'Device Groups' from the options.
- Click on the group name. The 'Create/Edit Device Group' interface for the selected group will open.

Home » Group devices

## Device Groups

<input type="checkbox"/>	ID	Group name	Os type	Creator user	Time creation
<input type="checkbox"/>	175	New Arrival for iOS		Yuliya	2014/08/20 03:49:54 PM
<input type="checkbox"/>	173	New Arrival for Android		Yuliya	2014/08/20 03:42:37 PM
<input type="checkbox"/>	169	Marketing Android Department		Yuliya	2014/08/20 03:27:10 PM
<input type="checkbox"/>	156	test_ios_dg		greg	2014/05/27 07:01:20 PM
<input type="checkbox"/>	154	test_and_c		greg	2014/05/27 06:56:36 PM
<input type="checkbox"/>					2014/05/22 07:24:56 PM
<input type="checkbox"/>					2014/05/22 05:01:59 PM

Home » Group devices » Create

### Create/Edit Device Group

Select devices to become members of a device group.

Group name \*

<input type="checkbox"/>	name
<input type="checkbox"/>	New iOS device
<input checked="" type="checkbox"/>	iPhone5 - Blue
<input type="checkbox"/>	iPhone 4s(Comodo)

Results per page: 20

- To change the name of the group, directly edit the name in the 'Group name' text box.
- To add new device(s) to the group, select the device(s) from the list.
- To remove device(s) from the group deselect the device(s) from the list.
- Click 'Save' for your changes to take effect.

If a new device is imported into a group, the configuration profiles in effect on the group will be applied to the device.

If a device is removed from a group, the configuration profiles in effect on the device because of association with the group, will also be removed.

### 5.2.3. Assigning Configuration Profile to Groups

The 'Devices Groups' interface allows the administrator to view the current configuration profiles applied to a device group and to apply new configuration profile to them.

For more details on profiles, refer to the chapter [Managing Configuration Profiles and Apps](#).

**To view and manage the profiles applied to a group**

- Open the 'Devices Groups' interface by clicking the 'Inventory' tab from the left hand side and choosing 'Device Groups' from the options.
- Select the group.
- Click the 'Manage Profiles' button.

The 'Manage Profiles for Android (or iOS) Device Group(s)' interface will open displaying all the configuration profiles available for group. Configuration profiles that is associated with the device group will be displayed with the check box beside it selected.

The screenshot shows the 'Device Groups' interface. At the top, there is a breadcrumb 'Home » Group devices'. Below it is a header 'Device Groups' with a mobile device icon. A table lists device groups with columns for ID, Group name, Os type, Creator user, and Time creation. The row for 'Marketing iOS Devices' (ID 17) is selected, with a red circle around its checkbox. Below the table is a 'Results per page' dropdown set to 20. Three buttons are visible: 'Manage Profiles' (circled in red), 'Create Android device group', and 'Create iOS device group'. A red arrow points from the 'Manage Profiles' button to a sub-interface titled 'Manage Profiles for iOS Device Group(s)'. This sub-interface shows the 'Device Group: Marketing iOS Devices' and a list of profiles with checkboxes. The 'name' profile is selected. At the bottom of the sub-interface are 'Results per page' (set to 20) and a 'Save' button.

<input type="checkbox"/>	ID	Group name	Os type	Creator user	Time creation
<input type="checkbox"/>	175	New Arrival for iOS	Apple	Yuliya	2014/08/20 03:49:54 PM
<input type="checkbox"/>	173	New Arrival for Android	Android	Yuliya	2014/08/20 03:42:37 PM
<input type="checkbox"/>	169	Marketing Android Department	Android	Yuliya	2014/08/20 03:27:10 PM
<input checked="" type="checkbox"/>	17	Marketing iOS Devices	Apple	Smith	2013/11/07 10:21:21 AM

Results per page: 20

**Manage Profiles** Create Android device group Create iOS device group

### Manage Profiles for iOS Device Group(s)

Device Group: Marketing iOS Devices

<input checked="" type="checkbox"/>	name
<input type="checkbox"/>	New Enrollment Profile
<input type="checkbox"/>	test iOS
<input type="checkbox"/>	kirill
<input type="checkbox"/>	Maintenance Department
<input type="checkbox"/>	Smith
<input type="checkbox"/>	New iOS profile
<input type="checkbox"/>	Smith
<input type="checkbox"/>	forTestiOSProfileAssociation
<input type="checkbox"/>	CoolWiFi
<input type="checkbox"/>	Kirill iOS
<input type="checkbox"/>	APN profile

Results per page: 20

Save

- To add a profile to the device group, select it from the list.
- To remove a profile from the device group, deselect it.

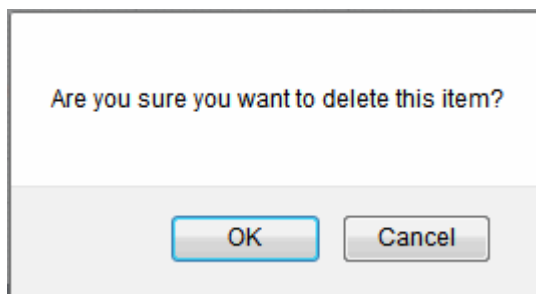
- Click the 'Save' button at the bottom for your changes to take effect.

### 5.2.4. Removing a Device Group

The administrator can remove a device group from the Device Groups interface.

#### To remove a device group

- Open the 'Device Groups' interface by clicking the 'Inventory' tab from the left hand side and choosing 'Device Groups' from the options.
- Click on the 'Delete' button **X** at end of the device group row. A confirmation dialog will appear.



- Click 'OK'. The device group will be removed from CMDM.

## 5.3. Managing Users


The Users interface allows new users to be added to Comodo Mobile Device Manager (CMDM). The users can be assigned with various roles with different privilege levels like administrators or end users. The mobile devices belonging to the endusers, can be enrolled into CMDM for remote and centralized management, only after adding the users to CMDM.

**Tip:** The roles with different access control settings, that can be assigned to the users added through this interface, can be managed through the Roles interface accessible by clicking 'Settings' from the left hand side and selecting Role Management. Refer to the section **Configuring the Role-Based Access Control for Users** for more details.



To open the Users interface, click the Inventory tab from the left hand side navigation and choose 'Users' from the options.

The Users interface displays the list of users that are added to CMDM. You can navigate through the successive pages using the 'Go to page' options at the bottom of the interface.


The screenshot shows the 'Users' management page in the Comodo Mobile Device Management interface. The page title is 'Home » Users'. Below the title, there is a 'Create User' button and a table listing existing users. The table has the following columns: ID, Username, Email, Phone number, Last login, Token Expire, Token Left, Token Status, # of Devices, and Mail Access. Three users are listed: Mallow (ID 2970), Jack (ID 2969), and Snowman (ID 2968). Below the table, there are controls for 'Results per page' (set to 20), 'Manage Profiles', 'Send tokens', and a field for '# of new device(s)' (set to 1). There are also buttons for 'Deny access to mailbox' and 'Allow access to mailbox'.

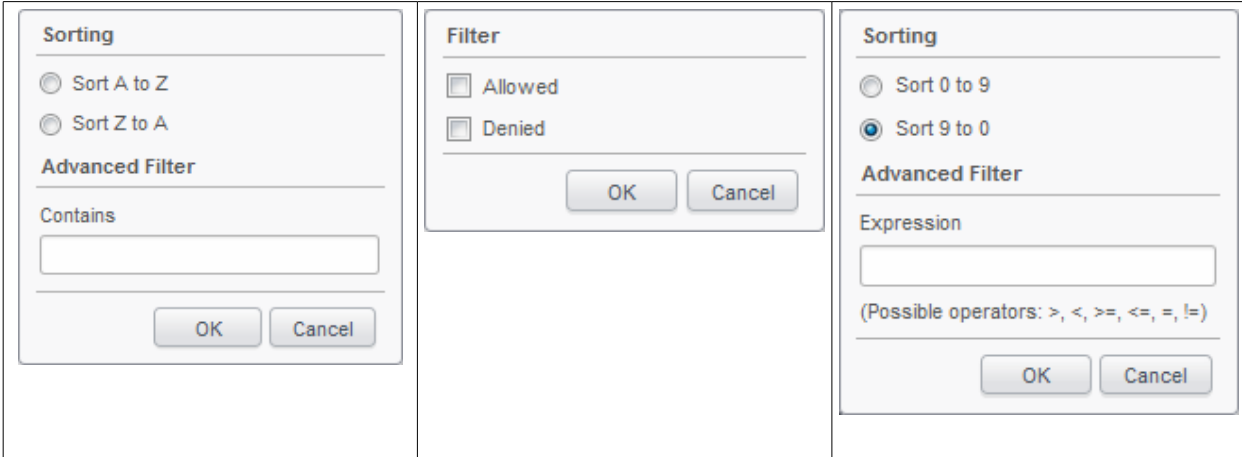
Users - Column Descriptions	
Column Heading	Description
ID	The Identity Number assigned to the user.
Username	The Login username of the user.
Email	The registered email address of the user.
Phone Number	The registered phone number of the user.
Last Login	Indicates the date and time of the users last login session.
Token Expire	Indicates the date and time when the token will expire. Tokens are sent to users via registered email at the time of user registration and during increasing the number of devices that a user can enroll for his / her account.
Token Left	Indicates the remaining number of devices left that a user can enroll for his / her account.
Token Status	Indicates the status of the token. The token sent via registered email is time restricted and should be used within 72 hours from receiving it for enrolling devices. <ul style="list-style-type: none"> <li>Active – The token is still active and can be used to enroll devices if the count is available.</li> <li>Expired – The validity of the token has expired.</li> <li>No Enrollments Left – The token has been used for all the devices allotted for the user.</li> <li>Not created – Only the user has been created and the number of devices that the user can enroll is not configured.</li> </ul>
# of Devices	Indicates the remaining number of devices that can be enrolled for the user.
Mail Access	Indicates a user access status to mailbox including all devices associated with a current user. Refer to <b>Configuring User Access To Mailbox</b> for more details.
Control Buttons	 Enables the administrator to view the details of the user. Refer to <b>View the details of a user</b> for more details.



	Enables the administrator to edit and update the details and reset the password of the user. Refer to <b>Updating Details of a User and Resetting Password</b> for more details.
	Enables the administrator to remove the user. Refer to <b>Removing a User</b> for more details.

## Sorting, Search and Filter Options

- Clicking a funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The Users interface allows the administrator to:

- Create a new user and enrolling their devices**
- View the details of a user**
- Edit/Update the details of the user and reset the password of a user**
- Assign configuration profile to a user**
- Add Devices for enrollment**
- Configuring User Access To Mailbox**
- Remove a user**

### 5.3.1. Creating New Users and Enrolling their Devices

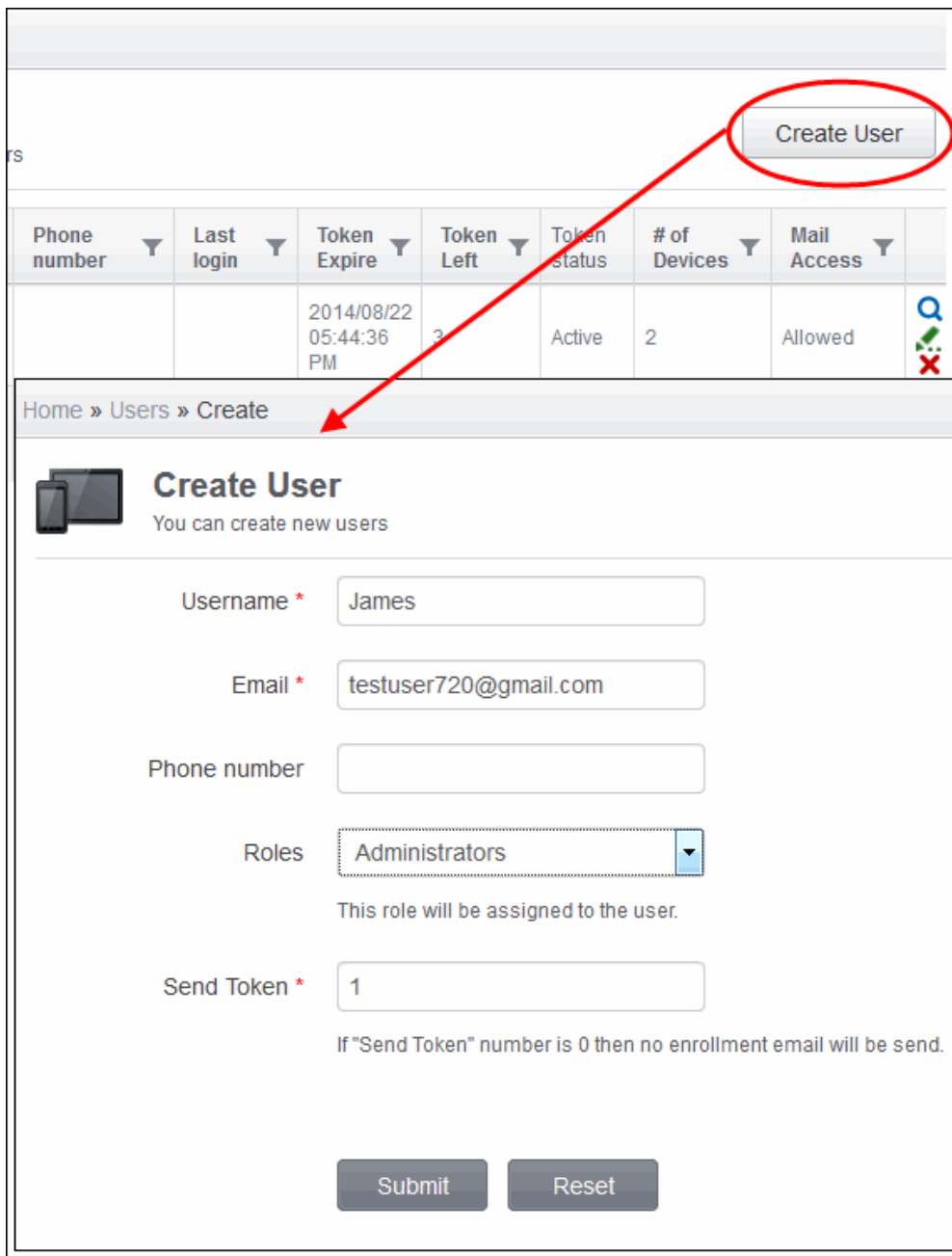
The administrators for CMDM and the users whose mobile devices are to be managed can be added to CMDM, through the Users interface. The Administrative or User roles can be assigned to the users during creation. On successful creation of new users / administrators, two emails will be sent to them, one for activating and setting password for accessing CMDM interface and another one containing token (pin code) for enrolling their devices.

**Important Note:** The devices belonging to/used by the users can be enrolled for centralized management to CMDM, only after the user is enrolled into the system. CMDM allows up to five devices for a single user. The number of users that can be added for an account depends on the license purchased. If the administrator needs to add more number of users than that covered by the license, they can upgrade their account by purchasing additional licenses. Refer to the section **Upgrading or Renewing**

the Licenses for more details.

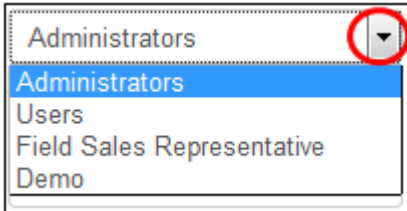
### To add a new user

- Click the 'Create User' button at the top right of the Users interface.



The Create User interface will open.

Create User Form – Table of Parameters		
Form Element	Type	Description
Username	Text Field	Enter the login username for the user.
Email	Text Field	Enter the email address of the user to which the device enrollment CMDM account activation procedures will be sent.
Phone Number (Optional)	Text Field	Enter the phone number of the user.

Create User Form – Table of Parameters		
Roles	Drop-down	<p>Select the role to be assigned to the new user from the drop-down.</p>  <p>The drop-down lists the Roles with different access control and privilege levels, as created through the Settings &gt; Role Management interface. Refer to the section <b>Configuring the Role-Based Access Control for Users</b> for more details.</p>
Send Token	Text Field	<p>Enter the number of devices that could be enrolled in CMDM by the user for his account. The maximum number of devices that could be enrolled for a user is five. If the number entered here is three, this can be increased to four or five later on. If the number is zero, then device enrollment mail will not be sent. Refer to the section <b>Adding Devices for Enrollment</b> for more details.</p>


- Enter the details, select the role for the new user and click the 'Submit' button.

**Tip:** The role assigned to the user can be changed at any time later, from the Settings > Role Management interface. Refer to the section **Managing Roles Assigned to a User** for more details.

The user will be added to CMDM and the user's details will be displayed.

Home » Users » User Info: James

---



## View User: James

---

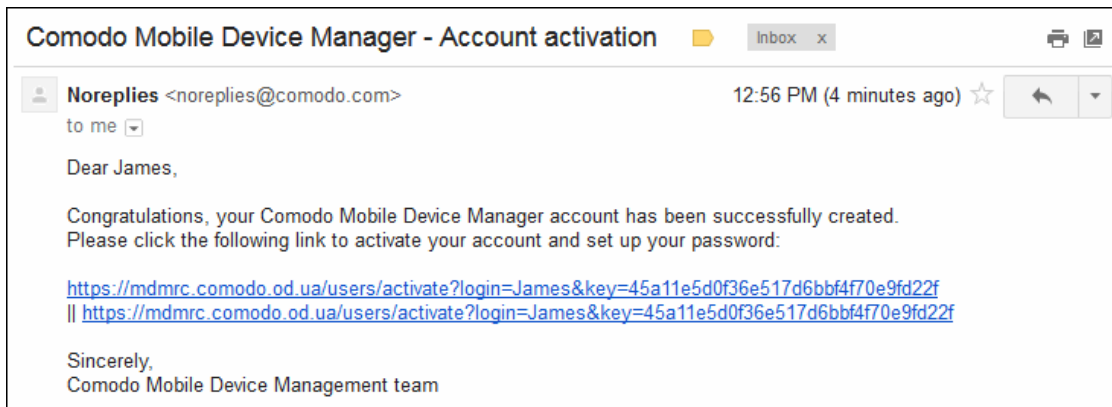
**Update**

ID	2975
Username	James
Email	<a href="mailto:testuser720@gmail.com">testuser720@gmail.com</a>
Phone number	
User created	2014/08/20 01:56:23 PM
Last login	Not set
Token Expire	2014/08/23 01:56:23 PM
Token Left	1
Token status	Active
# of Devices	0
Change password time	1970/01/01 03:00:00 AM

If required the administrator can update the details of the user by clicking the Update link at the top left. Refer to **Updating Details of a User and Resetting Password** for more details.

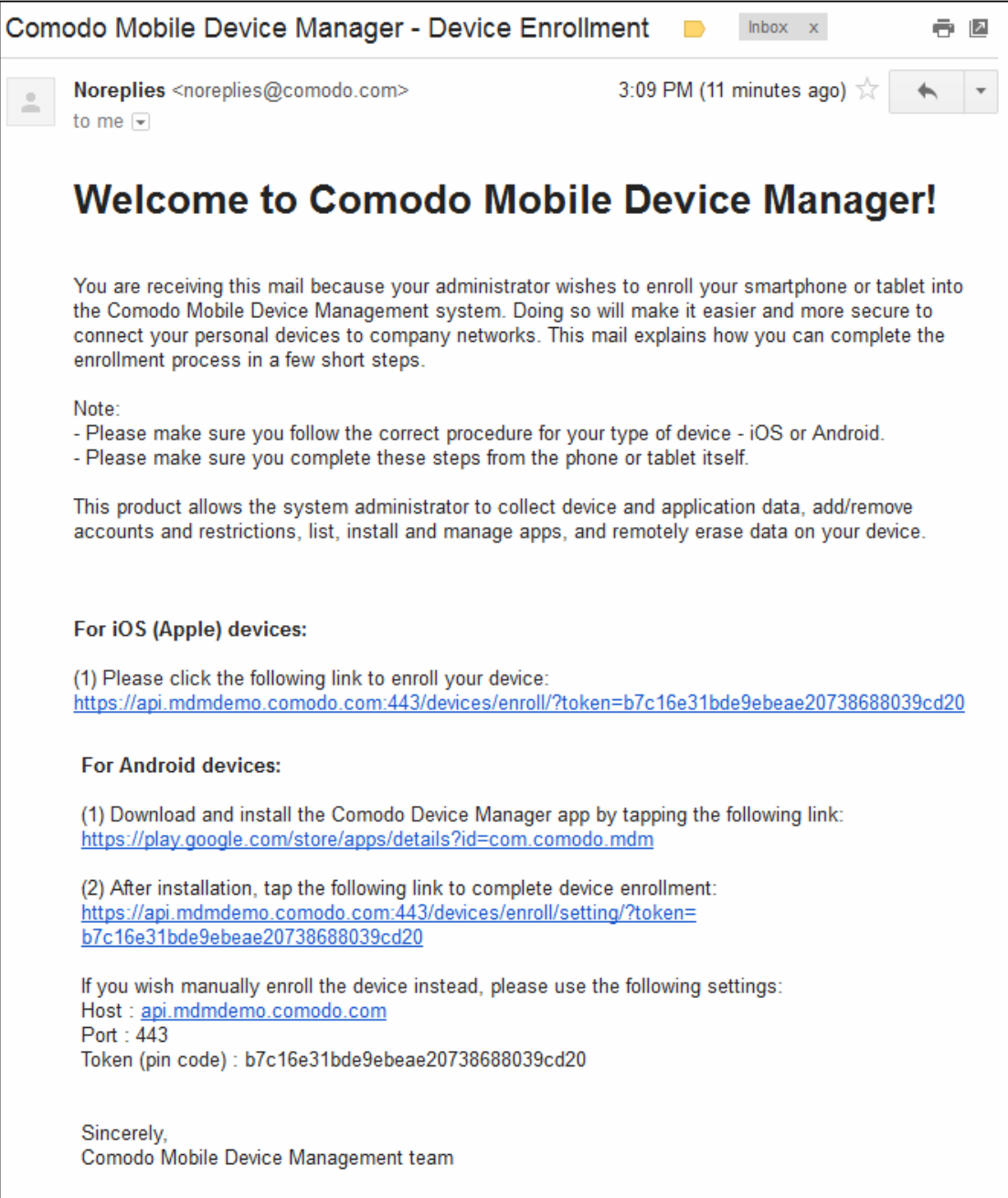
Once the user is added, an activation mail and device enrollment procedure email will be sent to the registered email address of the user. The user needs to activate the account and set the login password by clicking the 'Activate and set password' link in the activation email.

## Account Activation Email



Once activated, the user will be able to login to CMDM interface using the login username and password. The user's mobile devices can be enrolled to CMDM for management.

## Device Enrollment Email



Comodo Mobile Device Manager - Device Enrollment Inbox x

**Noreplies** <noreplies@comodo.com> 3:09 PM (11 minutes ago) ☆  
to me

## Welcome to Comodo Mobile Device Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone or tablet into the Comodo Mobile Device Management system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete the enrollment process in a few short steps.

**Note:**

- Please make sure you follow the correct procedure for your type of device - iOS or Android.
- Please make sure you complete these steps from the phone or tablet itself.

This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

**For iOS (Apple) devices:**

(1) Please click the following link to enroll your device:  
<https://api.mdm demo.comodo.com:443/devices/enroll/?token=b7c16e31bde9ebeae20738688039cd20>

**For Android devices:**

(1) Download and install the Comodo Device Manager app by tapping the following link:  
<https://play.google.com/store/apps/details?id=com.comodo.mdm>

(2) After installation, tap the following link to complete device enrollment:  
<https://api.mdm demo.comodo.com:443/devices/enroll/setting/?token=b7c16e31bde9ebeae20738688039cd20>

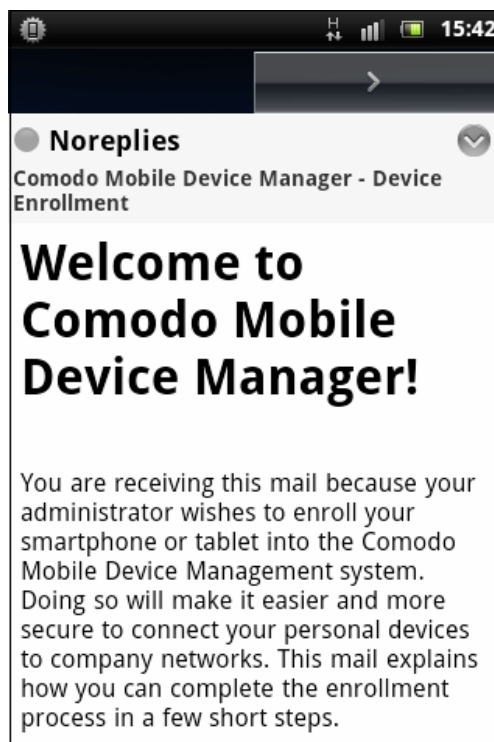
If you wish manually enroll the device instead, please use the following settings:  
 Host : [api.mdm demo.comodo.com](https://api.mdm demo.comodo.com)  
 Port : 443  
 Token (pin code) : b7c16e31bde9ebeae20738688039cd20

Sincerely,  
 Comodo Mobile Device Management team

The device enrollment email contain links to download the CMDM iOS Profiles and CMDM Android Agent with the enrollment instructions. Refer to next section **Adding Devices for Management** for more details. If you have left the **Count Enroll** field as 0, then the device enrollment email will not be sent. The mail will be sent only when you add devices for the user. Refer to the section **Adding Devices for Enrollment** for more details.

### 5.3.2. Adding Devices for Management

In order to centrally manage mobile devices, each device needs to be enrolled to Comodo Mobile Device Manager (CMDM). CMDM will send an email to the user containing enrollment instructions on successful creation of a user. The user should answer the email from the device (phone/tablet) to be enrolled.



CMDM allows to enroll up to five devices using the same token. The validity of the token is 72 hours and a new token should be generated for adding more devices after this period expires. Refer to the section **Adding Devices for Enrollment** for more details on how to generate emails containing enrollment token.

The following sections provide detailed explanations on enrolling devices with different Operating Systems.

- **Enrolling Android Devices**
- **Enrolling iOS Devices**

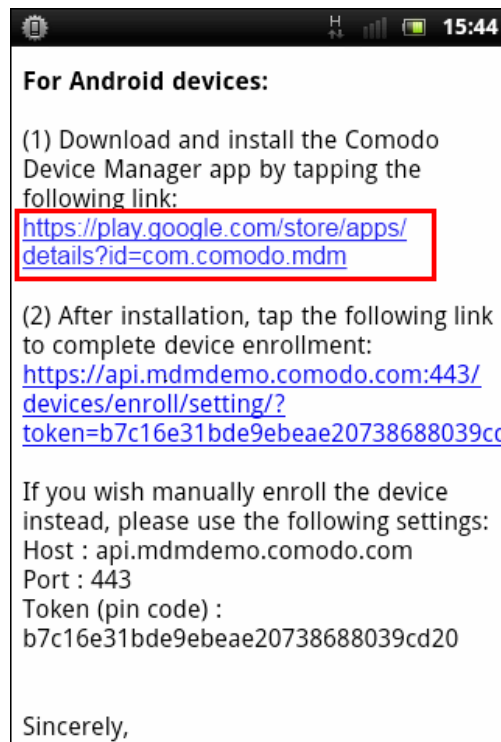
### 5.3.2.1. Enrolling Android Devices

After the administrator has created a user, he / she will receive an enrollment email with the link to download the android CMDM agent and a link to configure the agent. The user can follow the instructions in the mail and enroll the device in two steps.

- Step 1 - Downloading and Installing the agent
- Step 2 - Configuring the agent

#### **Step 1 - Downloading and Installing the agent**

- Open the mail in the device and tap the application download link under 'For Android devices'.



- You will be taken to the Google play store to download and install the agent.

## Step 2 - Configuring the agent

The agent can be configured to connect to the CMDM management server in two ways:

- **Automatic Configuration**
- **Manual Configuration**

### Automatic Configuration

- Tap the enrollment link contained in the email after the completion of installation.



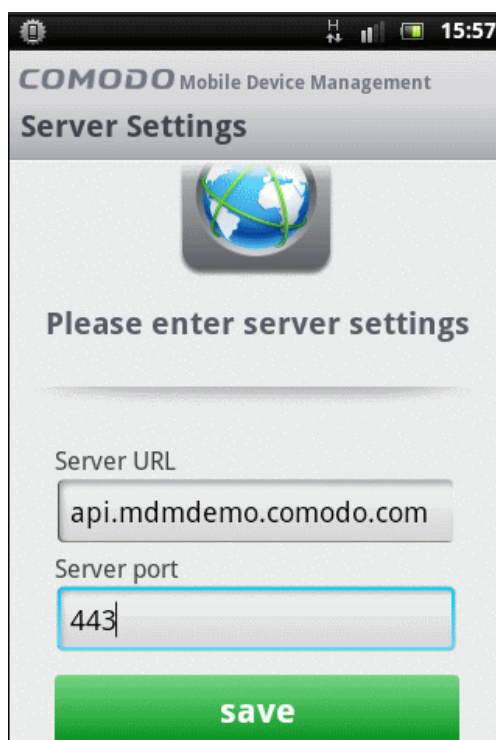


The agent will be automatically configured and the **End User License Agreement** screen will appear.

## Manual Configuration

- Open the agent by tapping the agent icon from your device. The agent configuration wizard will start enabling you to enroll the device by configuring the Server settings and unique PIN.

### Server Settings



Server Settings – Table of Parameters		
Form Element	Type	Description
Server URL	Text Field	Enter the url of the CMDM server contained in the mail. Usually this field is pre-populated.
Server port	Text Field	Enter the connection port of the server for your device to connect, as specified in the mail. Usually this field is pre-populated.

- Tap the 'save' button. The 'Login' screen will open

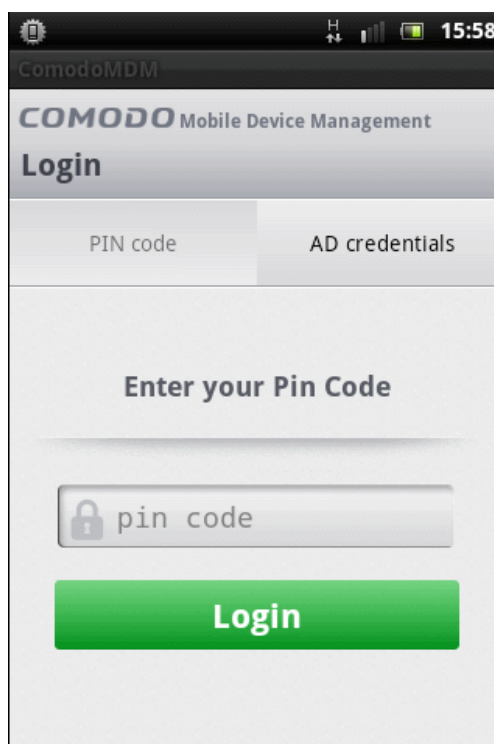
### Logging-in to the Console

You can make the app to login to the CMDM console in two ways:

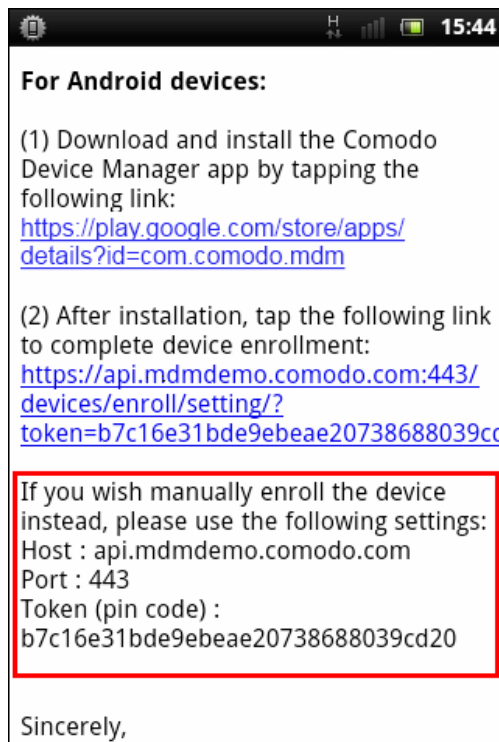
- **By entering the personal identification number (PIN) contained in the email**
- **By entering your username and password**

### Entering PIN

- Tap the 'Pin Code' tab in the 'Login' screen



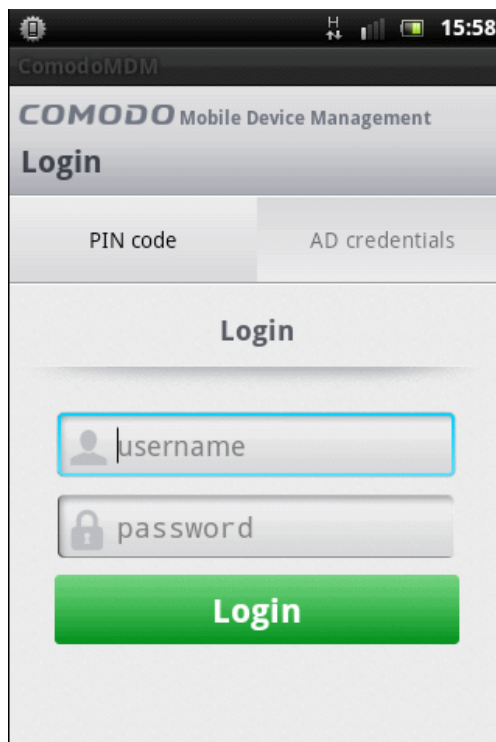
- Enter the PIN (token) contained in the enrollment email



- Tap 'Login'. The **End User License Agreement** screen will appear.

## Entering your username and password

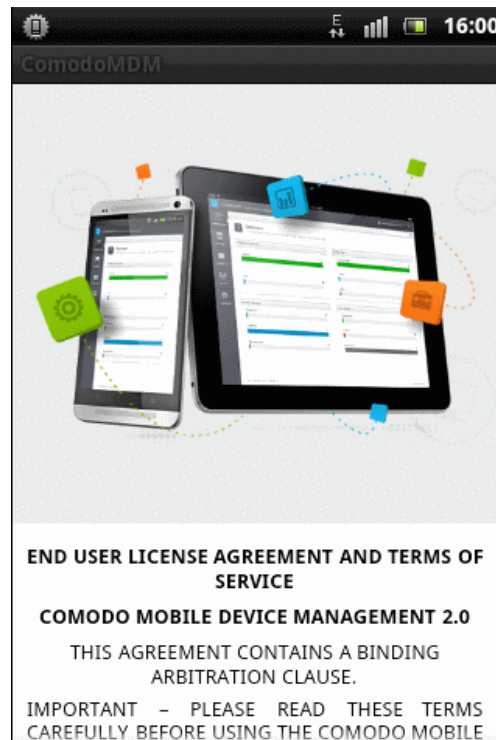
- Tap the '**AD Credentials**' tab in the 'Login' screen



- Enter your username contained in your account activation email and the password you set for your CMDM account.
- Tap the 'Login' button

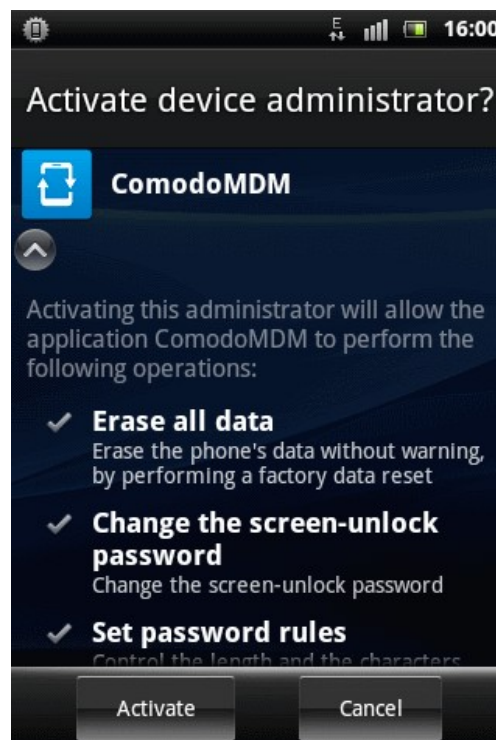
## End User License Agreement

The EULA screen will appear.

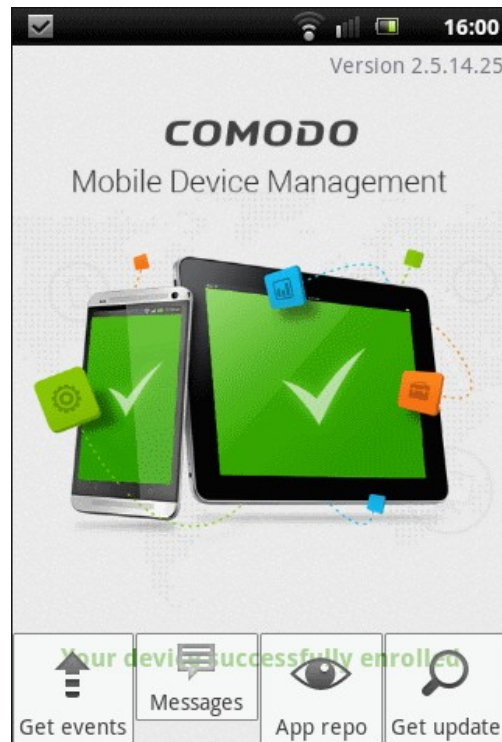


- Scroll down the screen, read the EULA fully and click the I Accept button at the bottom.

The Agent activation screen will appear.



- Tap 'Activate'.



The device is enrolled to CMDM and can be remotely managed from the CMDM console.

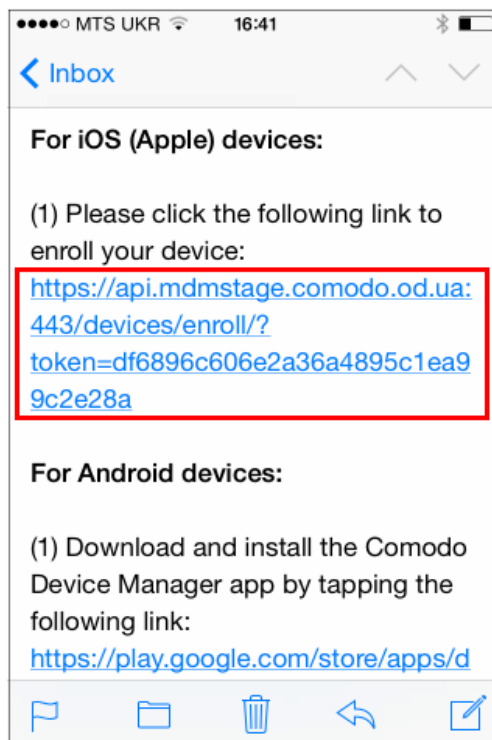
### 5.3.2.2. Adding iOS Devices

After the administrator has created a user, he / she will receive an enrollment email with the links to download the server certificate and the CMDM profile. The user can follow the instructions in the mail and enroll the device in two steps.

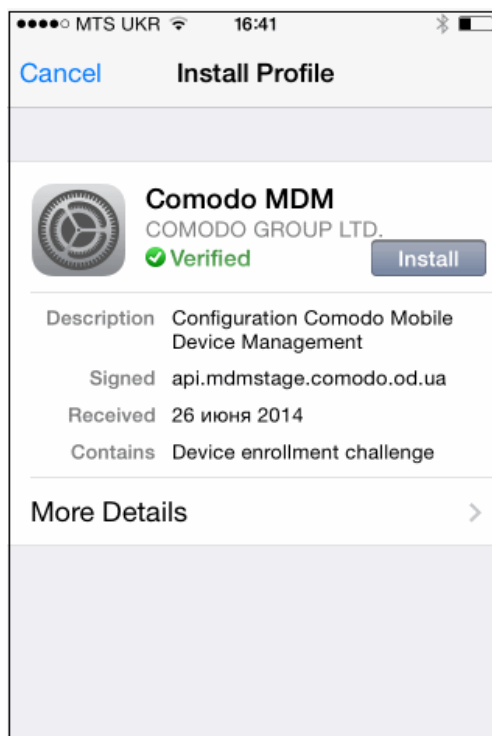
**Note:** The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

#### Installing the Certificate

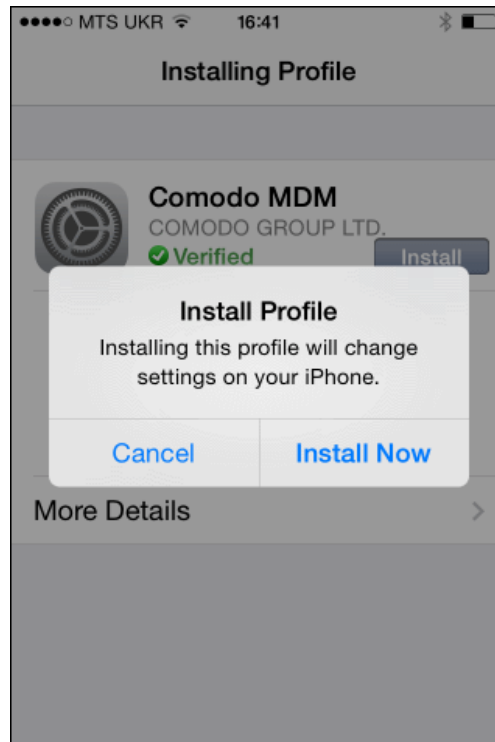
- Open the email on the device and tap the link under **For IOS only**



The 'Install Profile' wizard will start.

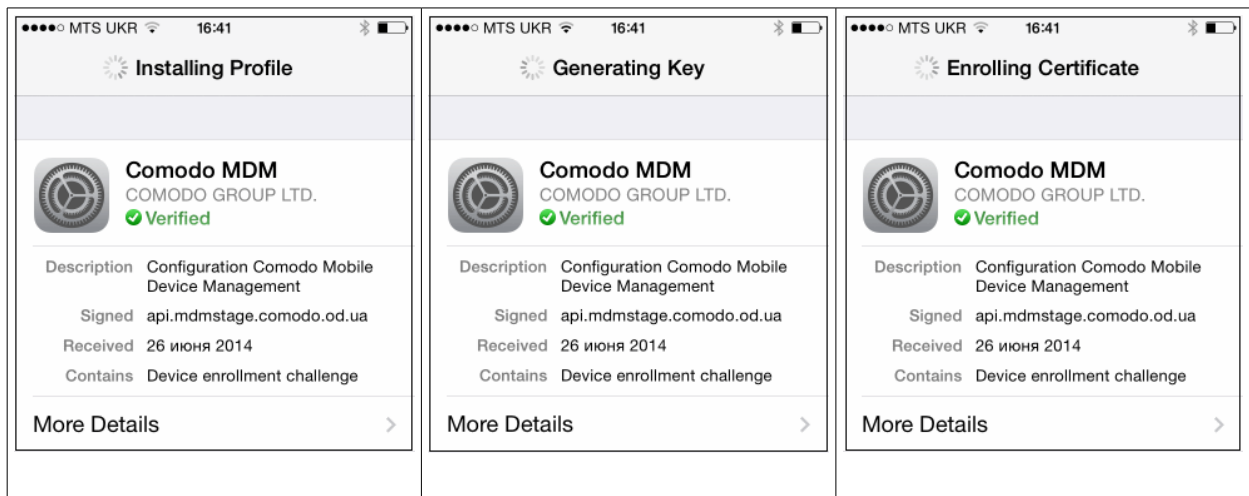


- Tap 'Install'. A confirmation dialog will be displayed.



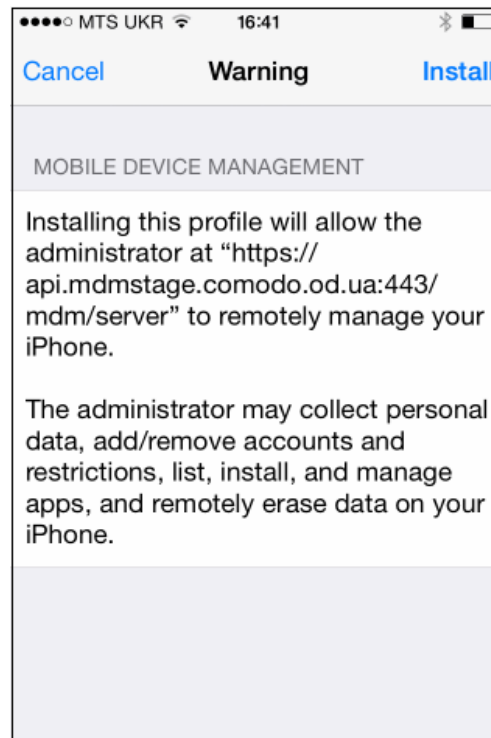
- Tap 'Install Now'.

The CMDM Profile installation progress will be displayed.

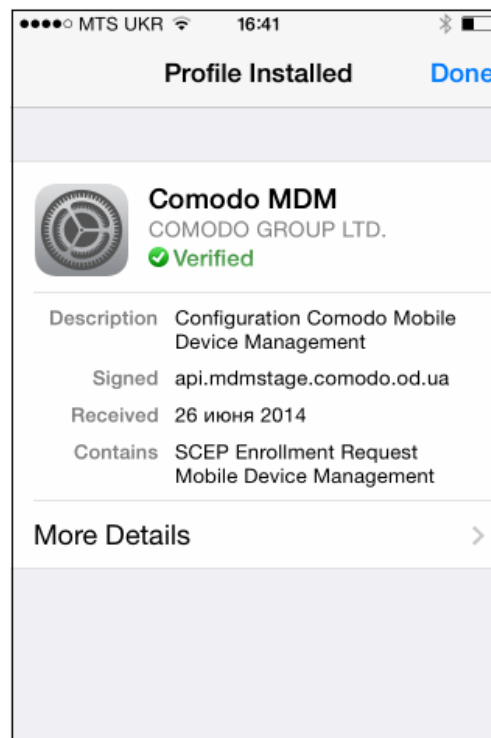


- A privacy warning screen with the privileges granted to the administrator by installing this profile will be displayed during the installation process. Read the warning fully and tap 'Install' to proceed.





The installation process will continue and when completed the 'Profile Installed' screen will be displayed.



- Tap 'Done' to finish the Comodo MDM profile installation wizard.

You can view the CMDM profile listed in the profiles screen of the device.

### 5.3.2.3. Downloading and Installing CMDM Client for iOS Devices

The iOS devices enrolled into CMDM for management as explained in the previous section '[Adding iOS Devices](#)' do not support some features such as apps management, GPS location and messaging. To get full functionality, users need to download CMDM client from iTunes website at <https://itunes.apple.com/us/app/cmdm/id807480077?mt=8>. CMDM client

supports iOS 6.0 and higher versions and is compatible with iPhone, iPad and iPod Touch.

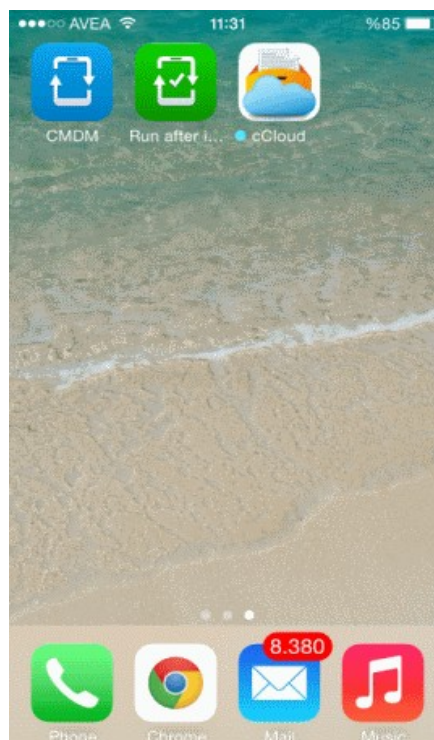
## To download and install CMDM client on iOS devices

- Visit the iTunes website at <https://itunes.apple.com/us/app/cmdm/id807480077?mt=8> and tap the CMDM icon

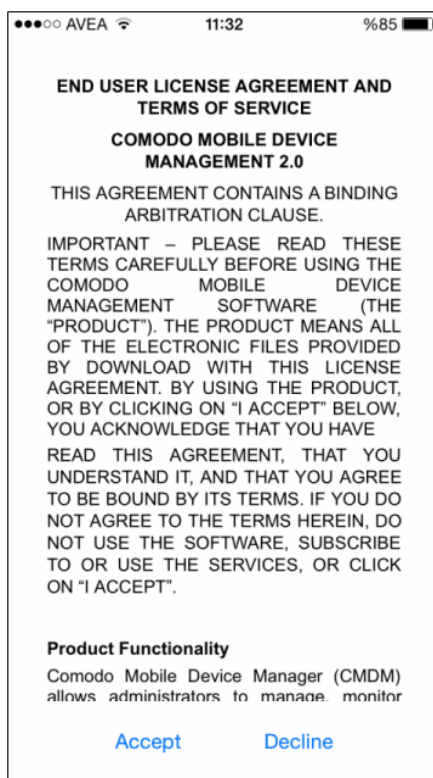


- Tap 'Install'

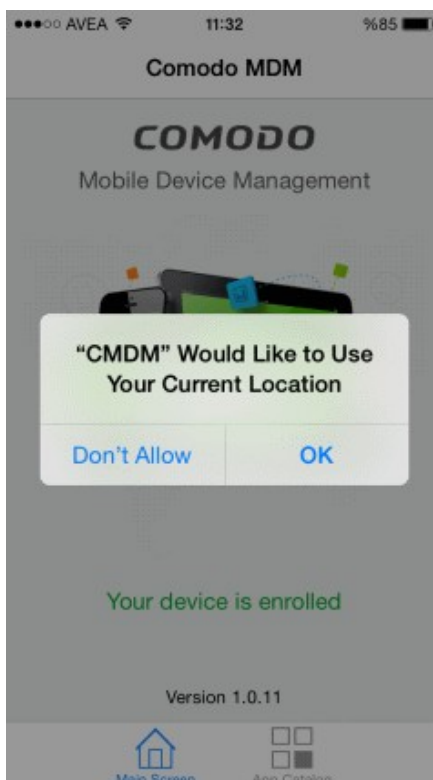
The CMDM app will be downloaded and installed on the device.



- Tap on the CMDM icon

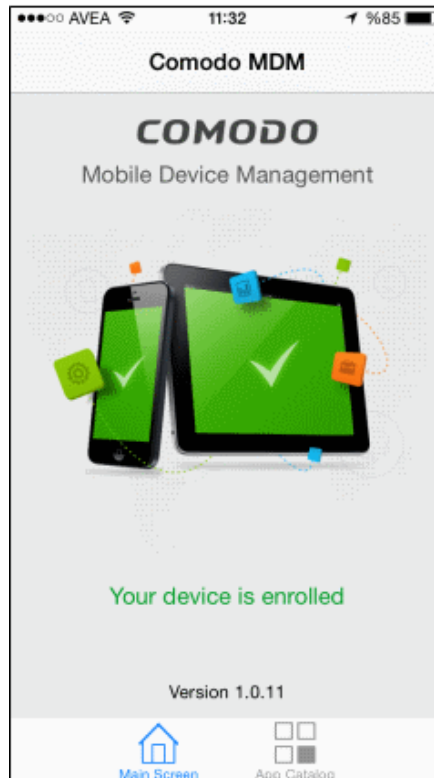


- Read the End User License Agreement fully and tap 'Accept'

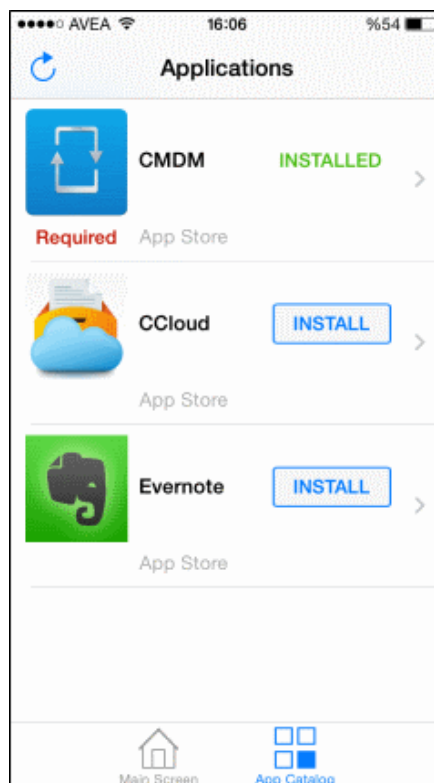


- Tap 'OK'.

The device will be successfully enrolled.




Tapping 'App Catalog' will display the iOS apps that are installed, required to be installed and available for installing. Refer the section Installing Apps on Devices for more details.




### 5.3.3. Viewing the Details of a User

The View User screen displays the details of a selected user.

#### To view the details

- Open Users interface by clicking Inventory > Users
- Click on the 'View' button  beside the selected user or simply click the name of the user

The View User screen will open.


Home » Users » User Info: James	
 <h2>View User: James</h2>	
<a href="#">Update</a>	
ID	2975
Username	James
Email	<a href="mailto:testuser720@gmail.com">testuser720@gmail.com</a>
Phone number	
User created	2014/08/20 01:56:23 PM
Last login	Not set
Token Expire	2014/08/23 01:56:23 PM
Token Left	1
Token status	Active
# of Devices	0
Change password time	1970/01/01 03:00:00 AM

The administrator can update the details of the user by clicking the Update link at the top left. Refer to [Updating Details of a User and Resetting Password](#) for more details.

### 5.3.4. Updating the Details of a User and Resetting Password

The administrator can update the login username, email address and phone number, and roles of a user at any time through Update User interface. The interface also allows the administrator to reset the password for the user, if required, e.g., if the user has forgotten the password and requests for password reset.

#### To update the details of a user

- Open Users interface by clicking Inventory > Users
- Click on the 'Update' button  beside the selected user

The 'Update User' interface will open.

Home » Users » James » Update

## Update User: James

Update user details and reset password

[Edit User's Roles](#) [Back to User Details](#) [Reset Password](#)

Username \*

Email \*

Phone number

[Save](#) [Reset](#)

- Edit the details directly as required and click 'Save'. The changes will be saved and take effect immediately.

### To reset the password for a user

- Click the 'Reset Password' button from the top right of the 'Update User' interface. A confirmation dialog will be displayed.

**Reset user's password?**

[OK](#) [Cancel](#)

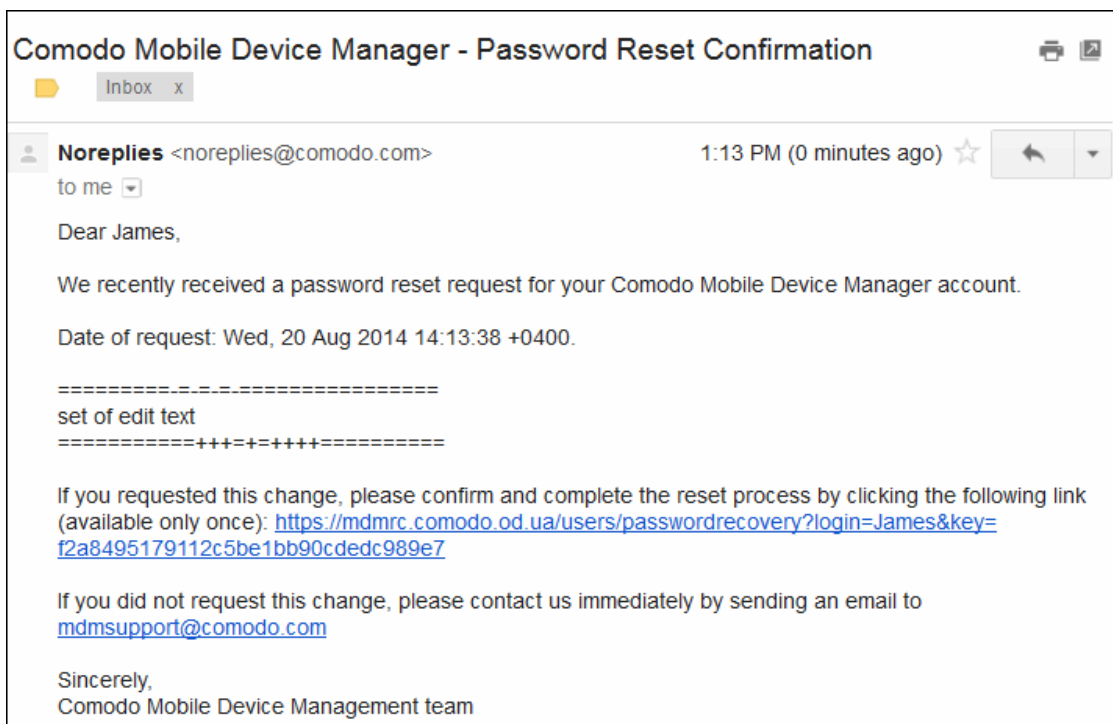
- Click 'OK'.

**Password has been reset.**

Prevent this page from creating additional dialogs

[OK](#)

- The password will be reset and a notification email will be sent to the user.



The user needs to click the 'Reset password' link in the mail and enter a new password in the resultant web page, in order to login to CMDM.

**To edit the roles of a user**

- Click the 'Edit User's Roles' button from the top right of the 'Update User' interface. The Edit Roles screen will be displayed. Refer to the section '**Managing Roles Assigned to a User**' for more details.

### 5.3.5. Assigning Configuration Profile to a User

CMDM allows administrators to assign profile(s) to user(s) so that the selected profiles will be deployed on all the devices associated with the user(s). This is particularly useful if organizations wants to roll out profiles to user-based devices.

**To assign configuration profile to a user**

- Click the 'Inventory' tab from the left hand side and choose 'Users' to open the 'Users' interface.
- Select the users for whom you want to assign profile(s).



Home » Users

## Users

Enroll new users and view/edit/assign profiles to existing users

<input type="checkbox"/>	ID	Username	Email	Phone number	Last login	Token Expire
<input checked="" type="checkbox"/>	2976	Bob	testuser720@gmail.com	919600142762		2014/08/23 02:21:42 PM
<input checked="" type="checkbox"/>	2975	James	testuser720@gmail.com			2014/08/23 01:56:23 PM

Results per page: 20

**Manage Profiles**    Send tokens    # of new device(s) 1

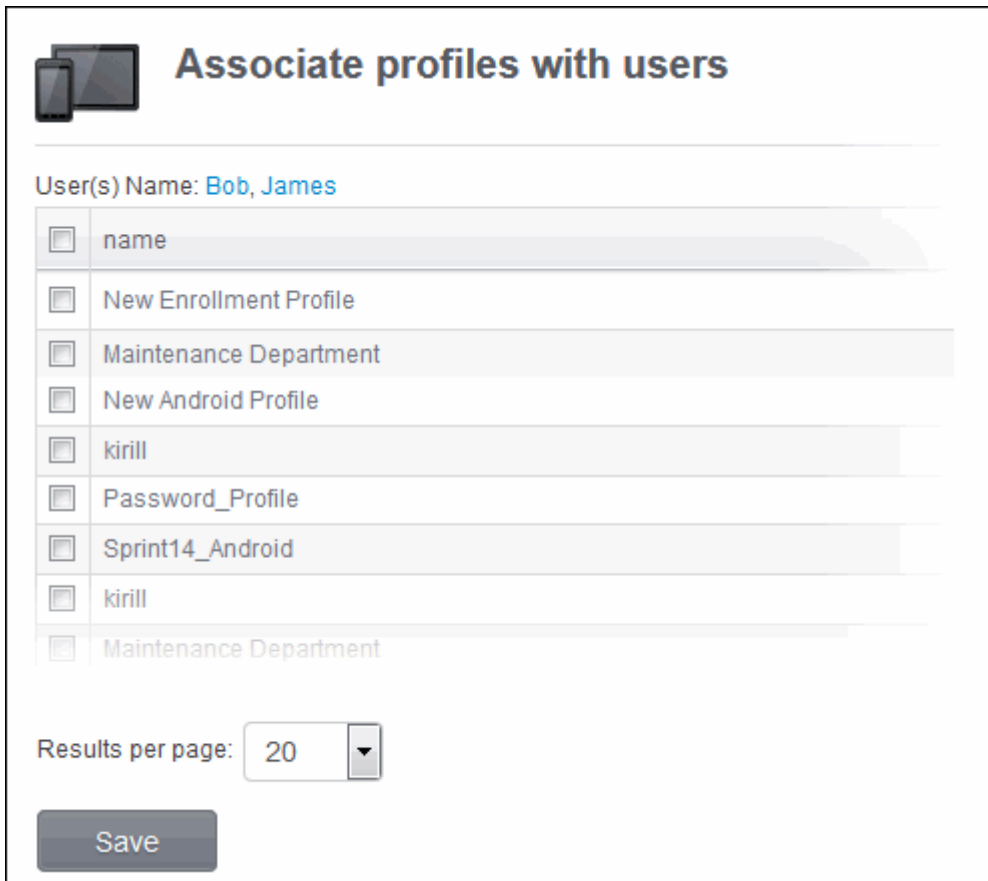
Total number of devices per user is limited to 5.

Deny access to mailbox

Allow access to mailbox

- Click the 'Manage Profiles' button.

The 'Associate profiles with users' interface will open.



**Associate profiles with users**

User(s) Name: **Bob, James**

<input type="checkbox"/>	name
<input type="checkbox"/>	New Enrollment Profile
<input type="checkbox"/>	Maintenance Department
<input type="checkbox"/>	New Android Profile
<input type="checkbox"/>	kirill
<input type="checkbox"/>	Password_Profile
<input type="checkbox"/>	Sprint14_Android
<input type="checkbox"/>	kirill
<input type="checkbox"/>	Maintenance Department

Results per page: 20

Save

- To add a profile to the user(s), select the checkbox beside the profile(s) from the interface.
- To remove profile(s) associated with users(s), deselect the checkbox beside the profile(s).
- Click 'Save' for your changes to take effect.

### 5.3.6. Adding Devices for Enrollment

CMDM allows users to enroll up to a maximum of five devices depending on the number allotted by the administrator. The number of devices that can be enrolled is entered at the time of **Creating a New User** or in the Users interface after creating a user. Please note that an administrator can only increase the number of devices that can be enrolled for a user and cannot decrease it. For example, if initially a user is allotted four devices that can be enrolled, an administrator can increase it to five later on but cannot decrease it to, say three or two. However, an administrator can remove an enrolled device from the Devices interface.

#### To add devices that can be enrolled

- Click the 'Inventory' tab from the left hand side and choose 'Users'.
- Select the user(s) for whom you want to add number of devices for enrollment.

Home » Users

## Users

Enroll new users and view/edit/assign profiles to existing users

<input type="checkbox"/>	ID	Username	Email	Phone number	Last login	Token Expire
<input type="checkbox"/>	2976	Bob	testuser720@gmail.com	919600142762		2014/08/23 02:21:42 PM
<input checked="" type="checkbox"/>	2975	James	testuser720@gmail.com			2014/08/23 01:56:23 PM
<input type="checkbox"/>	2974	super	super@mdm2013.net			2014/08/22 05:44:36 PM

Results per page: 20

Total number of devices per user is limited to 5.

- Enter the number of devices that can be enrolled in the '# of new devices(s)' field and click the 'Send tokens' button.
- If the user has not enrolled all the devices allotted and the validity period of the enrollment token has expired, click the 'Send tokens' button.

A MDM Device Enroll mail will be sent to the selected user(s), which contains the details such as number of devices that can be enrolled, procedure and token for enrolling devices and so on. Refer to the section '[Adding Devices for Management](#)' for more details.

### 5.3.7. Configuring User Access to Mailbox

After **installing the Exchange Service**, administrators can configure a user access to mailbox including all devices associated with the user.

#### To deny user access to mailbox

- Click the 'Inventory' tab from the left hand side and choose 'Users' from the options.
- Select the user whose device(s) are to be denied access.

Home » Users

## Users

Enroll new users and view/edit/assign profiles to existing users Create User

ID	Username	Email	Phone number	Last login	Token Expire	Token Left	Token status	# of Devices	Mail Access
2976	Bob	testuser720@gmail.com	919600142762		2014/08/23 02:21:42 PM	2	Active	0	Allowed
<input checked="" type="checkbox"/> 2975	James	testuser720@gmail.com			2014/08/23 01:56:23 PM	1	Active	0	Allowed

Results per page: 20

# of new device(s)

Total number of devices per user is limited to 5.

- Click the 'Deny access to mailbox' button.

The deny command will be sent. Once the command is successfully executed on the device, all devices associated with the user will be denied access to the mailbox in the Exchange server.

Access to mailbox for user is denied.

The status will display as 'Denied for user' under the Mail Access' column.

**Note:** All devices associated with a user will be blocked if IMEI of a device is not identified.

### To allow user access to mailbox

- Click the 'Inventory' tab from the left hand side and choose 'Users' from the options.
- Select the user that is denied access to mailbox.







The status of the user will be indicated as 'Denied for user' under the 'Mail Access' column.

- Click the 'Allow access to mailbox' button.

Home » Users

## Users

Enroll new users and view/edit/assign profiles to existing users Create User

<input type="checkbox"/>	ID	Username	Email	Phone number	Last login	Token Expire	Token Left	Token status	# of Devices	Mail Access	
<input checked="" type="checkbox"/>	2975	James	testuser720@gmail.com			2014/08/23 01:56:23 PM	1	Active	0	Denied	  
<input type="checkbox"/>	2976	Bob	testuser720@gmail.com	919600142762		2014/08/23 02:21:42 PM	2	Active	0	Allowed	  

Results per page: 20

Total number of devices per user is limited to 5.


- The allow command will be sent and after successful execution, the device(s) of the user can access mailbox.

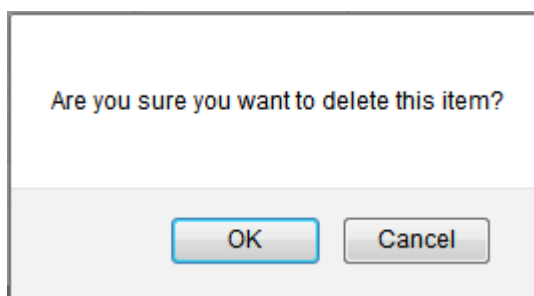
Access to mailbox for user is granted.

## 5.3.8. Removing a User

The administrator can remove a user and the device(s) associated with the user from the Users interface.

### To remove a user

- Open Users interface by clicking Inventory > Users
- Click on the 'Delete' button  beside the selected user. A confirmation dialog will appear.



- Click 'OK'. The user will be removed from CMDM.

**Note:** Once a user is removed the device(s) associated with the user will also be removed from CMDM. The configuration profiles applied to the user's device(s) by CMDM will also be removed from the devices.

## 5.4. Managing User Groups

Comodo MDM allows the administrator to create logical groups of users for convenient management of large number of users. For example, the users can be grouped as per the structure of the organization and/or depending on types of users. The administrator may create groups of users called 'Sales Department', 'Accounts Department' and so on.

Once created, the administrator can manage all users belonging to that group together. Dedicated configuration profiles can be created for each user group as per their requirements and the allowable user privileges and applied appropriately to them. For more details on creating and managing configuration profiles, refer to the chapter **Managing Configuration Profiles and Apps**.

User Groups can also be imported from Active Directory using LDAP. Once imported into the interface, the users in a group will be added to their respective only after they authenticate themselves using the LDAP credentials. Refer to the section **Importing User Groups** from LDAP for more details.

The 'User Groups' interface displays the list of user groups and allows the administrator to create new groups, edit a user group and assign configuration profiles to the groups as required.


To open the 'Group User' interface, click the 'Inventory' tab from the left hand side navigation and choose 'User Groups' from the options.

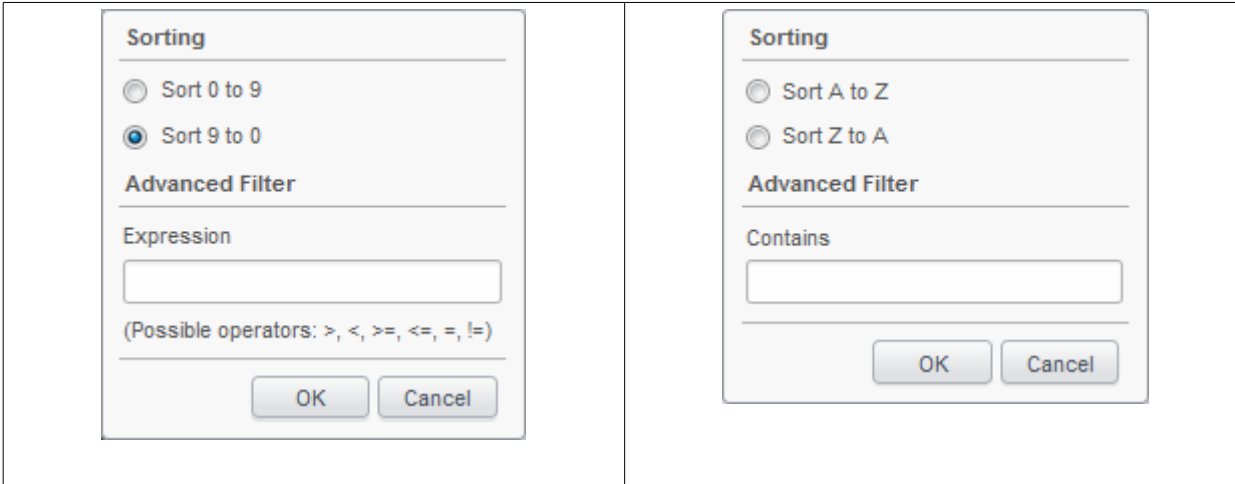
The screenshot shows the 'Group users list' interface. The table contains the following data:

ID	Group name	Creator user	Time creation	Last modified user	Control Buttons
105	testing	stepan	2014/08/15 01:56:08 PM	stepan	✗
104	Testets	greg	2014/07/23 05:39:12 PM		✗
103	Sprint14	greg	2014/07/22 01:43:19 PM	greg	✗
3	Smith	asli	2014/06/25 02:12:10 AM		✗

Group Users List - Column Descriptions		
Column Heading	Description	
ID	The Identity (ID) Number assigned to the user group.	
Group name	The name assigned to the user group by the administrator. Clicking the name of a group will open the 'Admin user group' interface that displays the list of users included in the group and allows you to add or remove devices to/from the group. Refer to the section <b>Editing a User Group</b> for more details.	
Creator User	Indicates the administrator that has created the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Time Creation	Indicates the date and time at which the group was created.	
Last Modified User	Displays the name of the administrator that has lastly edited the group. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the Administrator. Refer to the section <b>Viewing the details of the User</b> for more details.	
Control Buttons	✗	Enables the administrator to remove the group.
	Manage Profiles	Allows administrators to manage configuration profiles to selected user groups. Refer to the section <b>Assigning Configuration Profile to a User Group</b> for more details.
	Create user group	Allows administrators to create a new user group. Refer to the section <b>Creating a New User Group</b> for more

### Sorting and Filter Options

- Clicking a funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

From the Group User List interface, the administrator can:

- Create a New User Group**
- Edit a User Group**
- Assign Configuration Policy to User a Group**
- Remove a User Group**

#### 5.4.1. Creating a New User Group

Administrators can create user groups as required and add users into it. The grouping of users enables pushing selected configuration profiles to all the users pertaining to a group at-once.

##### To create a new user group

- Open the 'Group users list' interface by clicking the 'Inventory' tab from the left hand side and choosing 'User Groups'
- Click the 'Create user group' button at the bottom of the interface. The 'Admin user group' interface will open.




<input type="checkbox"/>	ID	Group name	Creator user	Time creation	Last modified user
<input type="checkbox"/>	105	testing	stepan	2014/08/15 01:56:08 PM	stepan
<input type="checkbox"/>	104	Testets	greg	2014/07/23 05:39:12 PM	
<input type="checkbox"/>	103	Sprint14	greg	2014/07/22 01:43:19 PM	greg
<input type="checkbox"/>	3	Smith	asli	2014/06/25 02:12:10 AM	

Results per page: 20 Displaying 1

Manage Profiles **Create user group**

Home » User groups » Create

 **Admin user group**  
You can create a new group with users.

Group name \*

<input type="checkbox"/>	login
<input type="checkbox"/>	Mallow
<input type="checkbox"/>	Jack
<input type="checkbox"/>	Snowman
<input type="checkbox"/>	John_Smith
<input type="checkbox"/>	admin

Results per page: 20

**Save**

The enrolled users are displayed in the screen.

- Enter the name to be assigned to the group in the 'Group name' text box.
- Select the user(s) that you want to import into the group. Note: You can add users at a later stage also.
- Click 'Save'. The new group will be created.

Group of users successfully created. ×

The new group will be listed in the 'Group users list' interface. Appropriate configuration profiles can now be applied to the new user group. Refer to [Assigning Configuration Policy to a User Group](#) for more details.

## 5.4.2. Editing a User Group

The administrator can view the users of a group and can add or remove users, from the 'User Groups' interface.

### To view and edit user groups

- Open the 'Group users list' interface by clicking the 'Inventory' tab from the left hand side and choosing 'User Groups' from the options.
- Click on the group name. The 'Admin user group' interface for the selected group will open displaying the users in the group preselected.

Home » Group users

## Group users list

<input type="checkbox"/>	ID	Group name	Creator user	Time creation	Last modified user	
<input type="checkbox"/>	107	Sales Department	Yuliya	2014/08/19 06:55:23 PM		✘
<input type="checkbox"/>	105	testing	stepan	2014/08/15 01:56:08 PM	stepan	✘
<input type="checkbox"/>	104	Testets	greg	2014/07/23 05:39:12 PM		✘
<input type="checkbox"/>	103	Sprint14	greg	2014/07/22 01:43:19 PM	greg	✘
<input type="checkbox"/>	3	Smith	asli	2014/06/25 02:12:10 AM		✘

Results per page: 20 Displaying 1-5 of 5 results.

[Manage Profiles](#) [Create user group](#)

Home » User groups » Create

## Admin user group

You can create a new group with users.

Group name \*

<input type="checkbox"/>	login
<input checked="" type="checkbox"/>	Mallow
<input checked="" type="checkbox"/>	Jack
<input checked="" type="checkbox"/>	Snowman
<input type="checkbox"/>	John_Smith
<input type="checkbox"/>	admin

Results per page: 20

[Save](#)

- To change the name of the group, directly edit the name in the 'Group name' text box.
- To add new user(s) to the group, select the checkbox beside the user(s) from the list.
- To remove user(s) from the group deselect the checkbox beside the user(s) from the list.
- Click 'Save' for your changes to take effect.

If a new user is imported into a group, the configuration profiles in effect on the group will be applied to the user's device.

If a user is removed from a group, the profiles in effect on the user's device because of association with the group, will also be removed.

### 5.4.3. Assigning Configuration Profile to a User Group

The 'User Groups' interface allows the administrator to view the current configuration profiles applied to a user group and to apply new configuration profile to them.

For more details on profiles, refer to the chapter [Managing Configuration Profiles and Apps](#).

#### To view and manage the profiles applied to a group

- Open the 'Group users list' interface by clicking the 'Inventory' tab from the left hand side and choosing 'User Groups' from the options.
- Select the group.
- Click the 'Manage Profiles' button.

The 'Association profiles on group users' interface will open displaying the profiles associated for the group preselected.

Home » Group users

### Group users list

<input type="checkbox"/>	ID	Group name	Creator user	Time creation	Last modified user	
<input checked="" type="checkbox"/>	107	Sales Department	Yuliya	2014/08/19 06:55:23 PM		✘
<input type="checkbox"/>	105	testing	stepan	2014/08/15 01:56:08 PM	stepan	✘
<input type="checkbox"/>	104	Testets	greg	2014/07/23 05:39:12 PM		✘
<input type="checkbox"/>	103	Sprint14	greg	2014/07/22 01:43:19 PM	greg	✘
<input type="checkbox"/>	3	Smith	asli	2014/06/25 02:12:10 AM		✘

Results per page: 20 Displaying 1-5 of 5 results.

**Manage Profiles** Create user group

### Association profiles on group users

Group users name: Sales Department

<input type="checkbox"/>	name
<input type="checkbox"/>	New Enrollment Profile
<input type="checkbox"/>	test iOS
<input type="checkbox"/>	New Android Profile
<input type="checkbox"/>	Smith
<input type="checkbox"/>	testAndroid
<input type="checkbox"/>	New iOS profile

- To add a profile to the user group, select the checkbox beside the profile from the list.
- To remove a profile from the user group, deselect the checkbox beside the profile from the list.
- Click 'Save' for your changes to take effect.


### 5.4.4. Removing a User Group

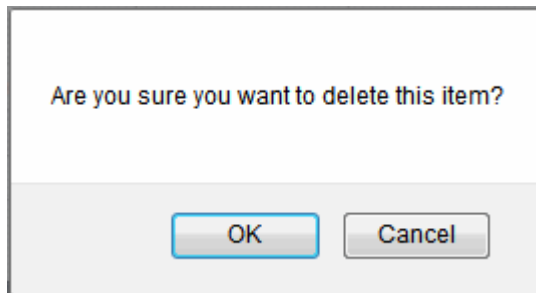
The administrator can remove a user group from the 'Group users' interface.

#### To remove a user group

- Open the 'Group users list' interface by clicking the 'Inventory' tab from the left hand side and choosing 'User Groups'

from the options.

- Click on the 'Delete' button  at end of the user group row. A confirmation dialog will appear.



- Click 'OK'. The user group will be removed from CMDM.

**Note:** Once a user group is removed, the profile(s) associated with the user group will also be removed from their devices and respective (Android or iOS) default profiles will be applied to their devices.

## 5.5. Managing Applications on Enrolled Devices

Comodo Mobile Device Manager (CMDM) provides visibility and control to the administrator over the applications installed on the users' devices. The 'Application Inventory' interface displays the list of applications identified from all the devices enrolled with CMDM. The administrator can determine authenticity of the applications and blacklist the applications found malicious, suspicious or not trustworthy. The blacklisted apps can be immediately blocked in the devices upon which they are installed and prevent from being installed on to other devices in future.

To open the 'Application Inventory' interface, click the Inventory tab from the left hand side navigation and choose 'Apps'.

Name	Package	Os type	# of Devices	Status
Compass-	7Z5K42C36D.CompassOne	Apple	2	Allowed
Compass	kr.sira.compass	Android	1	Allowed
Tip Tap	com.nikhil.tiptap	Android	0	Allowed
CMDM	42342342	Android	0	Allowed
Angry Birds Rio	com.rovio.angrybirdsrio	Apple	1	Allowed
wetre	124134	Apple	1	Allowed
Location Detector	com.baseman.locationdetector	Android	0	Allowed
K-9 Mail	com.fsck.k9	Android	0	Allowed
ImagePDFConversion 27-02-2012	demo.mypack	Android	0	Allowed
Image2pdf	ac.it.imgtopdf	Android	0	Allowed
Image to PDF Converter发布	com.Image_to_PDF_Converter_2	Android	0	Blacklisted
CMC Image Scanner	com.cmc.scan	Android	0	Allowed
Bluetooth File Transfer	it.medieval.blueftp	Android	0	Allowed
IQTest	com.vincesoft.iqtest	Apple	1	Allowed
Vision Test	com.threesidedcube.visiontest	Apple	1	Allowed
Music!	com.stubhub.svenues	Apple	0	Allowed
In the Kitchen	com.sni.iphone.applications.ITKApp	Apple	0	Allowed
Impossible	com.pixelcubestudios.moronquiz	Apple	1	Allowed
CMDM	com.comodo.mdm.client	Apple	0	Allowed
Ingress	com.google.ingress	Apple	0	Allowed

Go to page: 1 2 3 4 5 6 7 8 9 10 Next > Last >>


Results per page: 20

Displaying 1-20 of 686 results.

Buttons: Add to Black List, Remove from Black List, Inform devices now

Application List - Column Descriptions	
Column Heading	Description
Name	Name of the application.  The apps that are installed in some of the enrolled devices are displayed as links. Clicking the link opens the ' <b>Devices</b> ' interface listing only the devices on which the app is installed, enabling the administrator to identify the devices using the application.  The apps that were once installed in some of the devices and removed from all the devices later, are displayed as normal text.
Package	The package name or identifier of the package from which the app was installed.
OS Type	Indicates OS type of the app.
# of Devices	Indicates the number of devices on which the app is installed currently.
Status	Indicates whether the application is allowed or blacklisted.
Control Buttons	Add to Black List  Allows administrators to add selected apps to be added to blacklist. Refer to the section <b>Moving Selected Apps to Blacklist</b> for more details.
	Remove from Black List  Allows administrators to remove selected apps from the blacklist. Refer to the section <b>Unblocking Blacklisted Apps</b> for more details.
	Inform devices now  Allows administrators to execute the blacklist apps or remove from blacklist commands instantly.

## Sorting, Search and Filter Options

- Clicking a funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:

**Sorting**

Sort 0 to 9

Sort 9 to 0

**Advanced Filter**

Expression

(Possible operators: >, <, >=, <=, =, !=)

**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

Contains

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.

- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

From the Application list interface, the administrator can:

- **Move selected untrusted apps to blacklist and block the apps from devices**
- **Remove trusted apps from blacklist**

## 5.5.1. Moving Selected Apps to Blacklist

The Application Inventory interface displays all the apps that are installed or removed on all the enrolled devices. The administrator can analyze the list and if any suspicious or malicious application is identified, administrator can block the application in the devices in which they are installed and prevent other devices to install the application in future, by moving it to the blacklist.

### To move selected apps to blacklist

- Click the 'Inventory' tab from the left hand side and choose 'Apps' from the options.
- Select the apps to be black listed
- Click the 'Add to Black List' button.

The selected apps will be included to the Black List and their status will change to 'Blacklisted'

- To block the apps immediately in the devices on which they are installed, click the 'Inform devices now' button.

Home » Devices » Application list

### Application Inventory

<input type="checkbox"/>	Name	Package	Os type	# of Devices	Status
<input type="checkbox"/>	State Bank Anywhere	com.sbl.SBIFreedomPlus		1	Allowed
<input type="checkbox"/>	Data monitor	com.sonyericsson.android.datamonitor		0	Allowed
<input type="checkbox"/>	LiveWare™ manager	com.sonyericsson.extras.liveware		0	Allowed
<input type="checkbox"/>	VK	com.vk.vkclient		0	Allowed
<input type="checkbox"/>	Get To The Chopper	com.theinvisibleowl.gettothechopper		0	Allowed
<input type="checkbox"/>	Swing Copters	com.dotgears.swing		0	Allowed
<input type="checkbox"/>	mobile9+	com.mobile9.market		1	Allowed
<input checked="" type="checkbox"/>	Image2PDF	fts.image2pdf.demo		1	Allowed
<input type="checkbox"/>	beaming	com.beaming		1	Allowed
<input type="checkbox"/>	CMDM	123456		0	Allowed
<input type="checkbox"/>	VivaVideo	com.quvideo.xiaoying		0	Allowed
<input type="checkbox"/>	TrakAx	com.highandes.TrakAx		0	Allowed
<input type="checkbox"/>	Text Edit	org.paulmach.textedit		0	Allowed
<input type="checkbox"/>	Retrica	com.venticake.retrica		0	Allowed
<input type="checkbox"/>	Photo Editor	com.iudea.android.photo.editor		0	Allowed
<input type="checkbox"/>	Drum Pads 24	com.paulpnyaga.drumpads24		0	Allowed
<input type="checkbox"/>	BaldBooth	com.piviandco.baldbooth		0	Allowed
<input type="checkbox"/>	2048	com.presselite.the2048game		0	Allowed
<input type="checkbox"/>	CMDM	888888		0	Allowed
<input type="checkbox"/>	Shots	com.shots.android		1	Allowed

Go to page: 1 2 3 4 5 6 7 8 9 10 Next > Last >> Displaying 1-20 of 712 results.

Results per page: 20

## 5.5.2. Unblocking Blacklisted Apps

If an application is moved to blacklist by mistake or if an application previously blacklisted appears to be a genuine or trustworthy, the administrator can remove it from the blacklist and allow the application to be installed or run in the devices.

### To remove trustworthy apps from blacklist



- Click the 'Inventory' tab from the left hand side and choose 'Apps' from the options.
- Select the blacklisted apps to be unblocked.
- Click the 'Remove from Black List' button.

Home » Devices » Application list

### Application Inventory

<input type="checkbox"/>	Name	Package	Os type	# of Devices	Status
<input type="checkbox"/>	State Bank Anywhere	com.sbi.SBIFreedomPlus	Android	1	Allowed
<input type="checkbox"/>	Data monitor	com.sonyericsson.android.datamonitor	Android	0	Allowed
<input type="checkbox"/>	LiveWare™ manager	com.sonyericsson.extras.liveware	Android	0	Allowed
<input type="checkbox"/>	VK	com.vk.vkclient	iOS	0	Allowed
<input type="checkbox"/>	Get To The Chopper	com.theinvisibleowl.gettothechopper	Android	0	Allowed
<input type="checkbox"/>	Swing Copters	com.dotgears.swing	iOS	0	Allowed
<input type="checkbox"/>	mobile9+	com.mobile9.market	Android	1	Allowed
<input checked="" type="checkbox"/>	Image2PDF	its.image2pdf.demo	Android	1	Blacklisted
<input type="checkbox"/>	beaming	com.beaming	Android	1	Allowed
<input type="checkbox"/>	CMDM	123456	iOS	0	Allowed
<input type="checkbox"/>	VivaVideo	com.quvideo.xiaoying	Android	0	Allowed
<input type="checkbox"/>	TrakAx	com.highandes.TrakAx	Android	0	Allowed
<input type="checkbox"/>	Text Edit	org.paulmach.textedit	Android	0	Allowed
<input type="checkbox"/>	Retrica	com.venticave.retrica	Android	0	Allowed
<input type="checkbox"/>	Photo Editor	com.ludesk.android.photo.editor	Android	0	Allowed
<input type="checkbox"/>	Drum Pads 24	com.paulpnyagov.drumpads24	Android	0	Allowed
<input type="checkbox"/>	BaldBooth	com.piviandco.baldbooth	Android	0	Allowed
<input type="checkbox"/>	2048	com.presselite.the2048game	Android	0	Allowed
<input type="checkbox"/>	CMDM	888888	iOS	0	Allowed
<input type="checkbox"/>	Shots	com.shots.android	Android	1	Allowed

Go to page: 1 2 3 4 5 6 7 8 9 10 Next > Last >>

Results per page: 20

Displaying 1-20 of 712 results

Inform devices now

Add to Black List Remove from Black List

- If you want the changes to take effect immediately, click the 'Inform devices now' button.

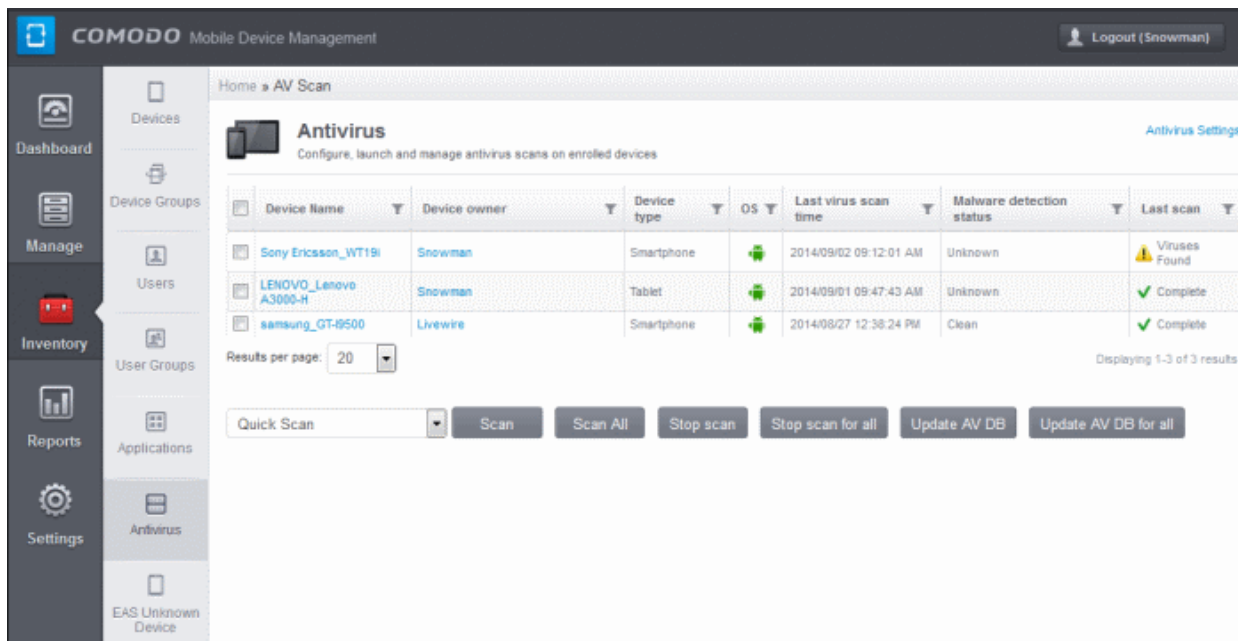
## 5.6. Managing Antivirus and Running Scans on Enrolled Devices

The administrator can initiate manual or on-demand antivirus scans on selected or all devices at-once and view the status of scheduled or on-demand scans from the 'AV Scan' interface. The interface also allows the administrator to update virus signature database on the devices.

**Tip:** The administrator can configure automatic or scheduled AV scans to be run periodically. The scan schedule can be created as a configuration profile and pushed to selected devices or groups of devices. Refer to the section **Creating Configuration Profiles** for more details. The infections identified after scheduled or on-demand scan will be treated as configured in the Antivirus Settings interface accessible by clicking Settings > Antivirus Settings. If 'Manual control' is chosen, then the administrators have the option to uninstall, ignore or move to quarantine in results displayed below the Antivirus screen. The scan results can also be viewed from the Threats Reports interface accessible by clicking 'Reports' tab from the left hand side.

To open the 'AV Scan' interface, click the 'Inventory' tab from the left hand side navigation and choose 'Antivirus'.



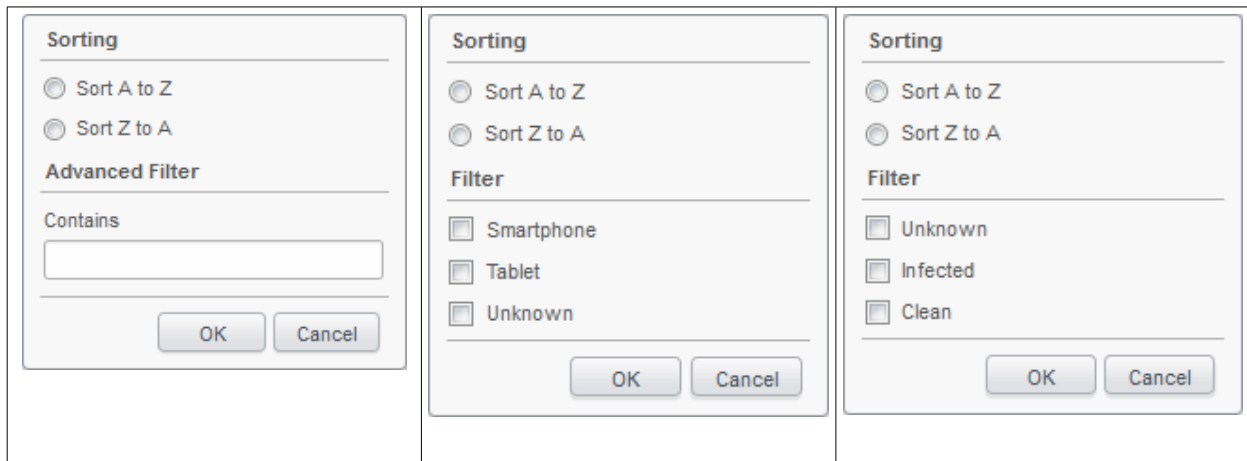


### AV Scan - Column Descriptions

Column Heading	Description
Device Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device. Clicking the name of the device will open the View Device interface that displays the complete details of the device and enables the administrator to locate the device and to apply configuration profiles. Refer to the section <b>Managing an Individual Device</b> for more details.
Device Owner	Name of the person owns the device as registered in CMDM.
Device Type	Indicates the type of the device
OS	Indicates the device's operating system.
Last Virus Scan Time	Indicates the date and time at which the last antivirus scan was run.
Malware Detection Status	Indicates whether the device is found infected or not, from the results of the last scan
Last Scan	Indicates the status of last run scan or currently running scan.

### Sorting, Search and Filter Options

- Clicking a funnel button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

The AV Scan allows the administrator to:

- **Run on-demand AV scan on selected or all device(s)**
- **Update virus signature database on selected or all device(s)**

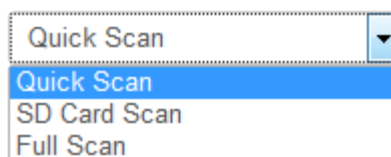
## 5.6.1. Running On-demand Antivirus Scans

The AV Scan interface allows the administrator to launch instant scans on selected device. Depending on the need the scans can be run for the whole device or on selected areas like critical areas containing the operating system files or the SD card mounted in the device. On completion of the scan, the infected applications, if identified, will be uninstalled, moved to quarantine or ignored as configured in the Antivirus Settings page.

**Tip:** The administrator can choose to manually remove or configure CMDM to automatically remove the infected items from the 'Antivirus Settings' page. If 'Manual control' is chosen, then the administrators have the option to uninstall, ignore or move to quarantine in the results displayed below the Antivirus screen. The settings interface can be accessed by clicking the 'Antivirus Settings' link at the top right of the AV Scan interface or by clicking Settings > Antivirus Settings. Refer to the sections **Antivirus Settings** for more details.

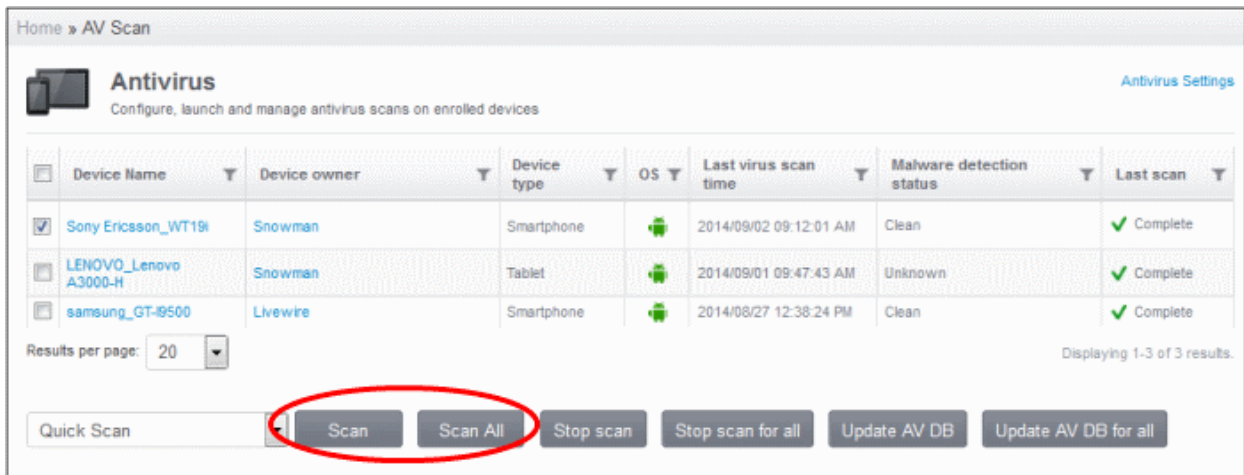
### To launch an on-demand AV scan

- Click the 'Inventory' tab from the left hand side and choose 'Antivirus'.
- If you want run the scan only on specific devices, select the devices. If you want to run the scan on all the devices, you need not select the devices.
- Select the scan profile that define the areas to be scanned from the drop-down at the bottom left.



- **Quick Scan** - Scans the critical areas of the device, which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include RAM, hidden services and other significant areas like system files. These areas are of great importance to the health of the device so it is essential to keep them free of infection.

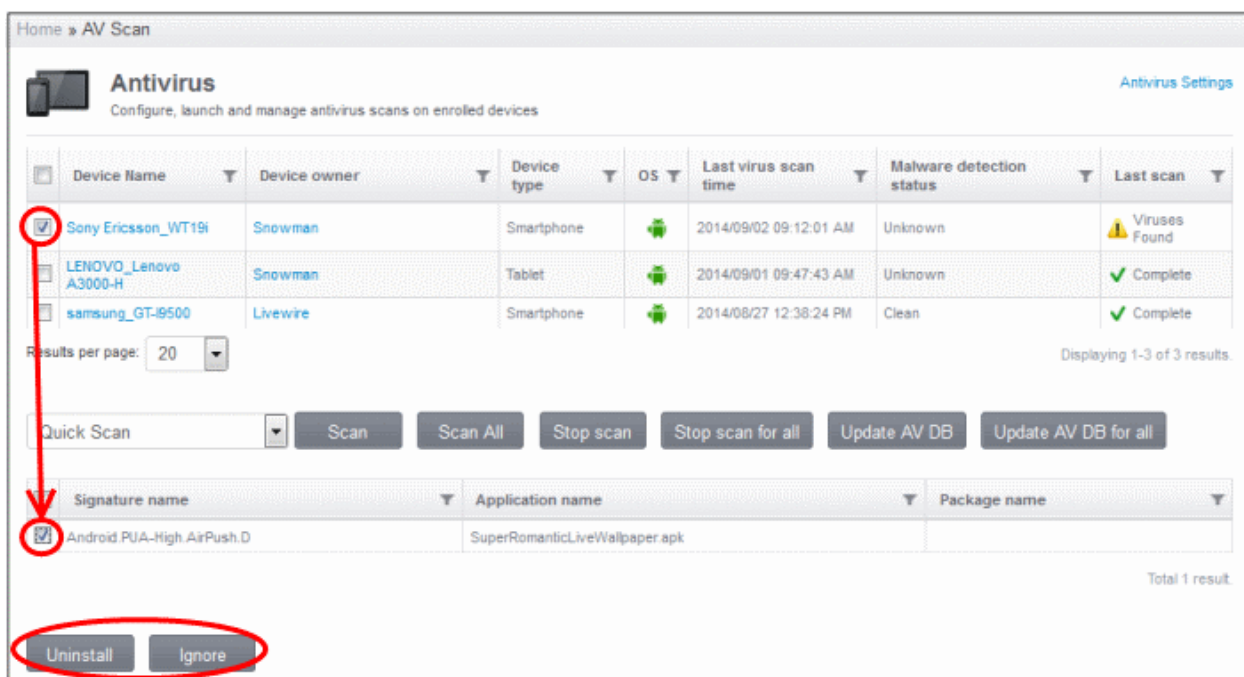
- **SD Card Scan** - Scans all folders/files in the Secure Digital (SD) memory card mounted on the device.
- **Full scan** - Scans all the folders/files in both the system internal memory and the SD card.
- If you want to run the scan on selected devices, click the Scan Selected button. If you want to run the scan on all the devices at-once, click the 'Scan All' button.



- If you want to terminate the scanning on selected devices, choose the devices and click the 'Stop Scanning for selected' button.
- If you want to terminate the AV scans from all the devices scanned presently, select the 'Stop Scan for all' button.

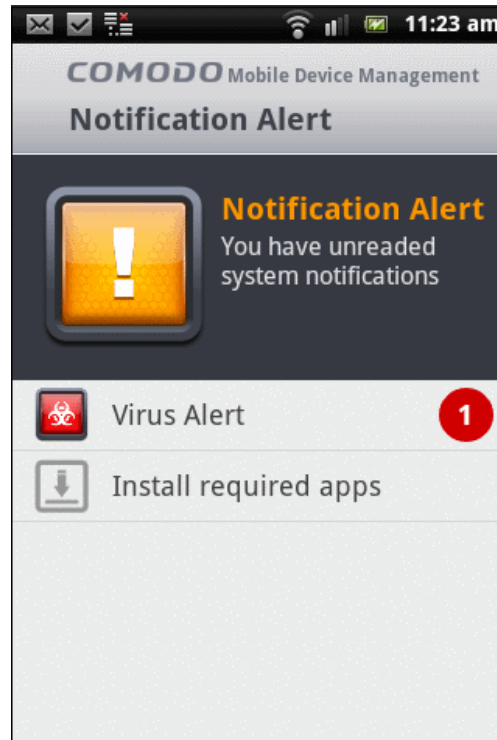
On completion of the scan, the result will be displayed in the 'Status' column of the same interface.

- If AV settings is configured to automatically uninstall or move the infected item to quarantine, the identified malicious item will be cleaned accordingly.
- If the AV settings is configured for manual removal of infections, and if any malware is found, the status column will display 'Viruses found'. The results will be displayed at the bottom of the interface on selecting the infected devices.

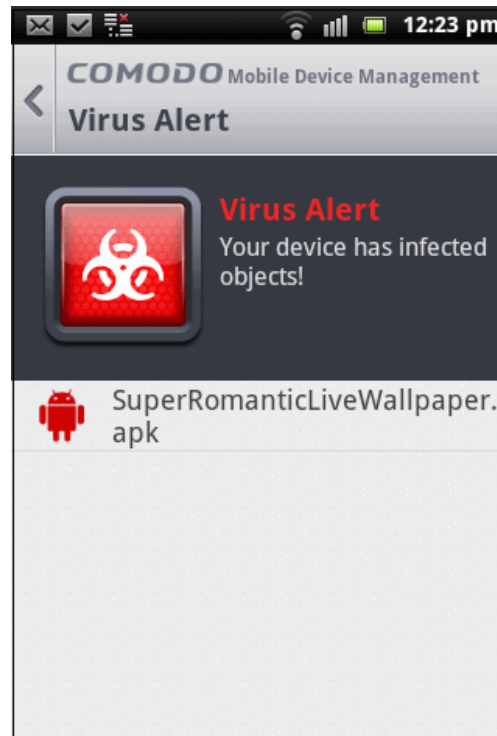


- Select the malware in the results screen, click either Uninstall or Ignore button.

A notification alert screen will also be displayed on the affected devices.



The notification screen will indicate the number of threats found in the device. On clicking the 'Virus alert' a summary of virus, push ads and unsafe apps in the device will be displayed. If apps infected with malware are found, the 'Remove virus' button will be displayed.



The user needs to tap on the malware to be removed and confirm to remove malware in the next dialog to uninstall the app containing the malware.



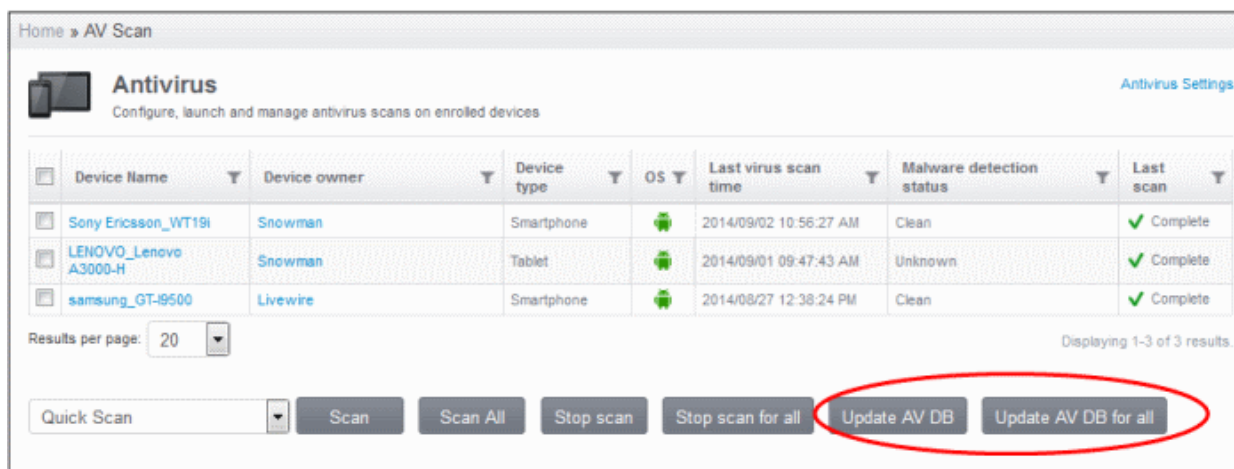
## 5.6.2. Updating AV Databases on Devices

In order to guarantee continued and effective antivirus protection, it is imperative that the virus signature databases on the devices are updated as regularly as possible.

CMDM automatically downloads periodical updates from the update server and installs them on the devices. However, if the device was not in connection for sometime, it might have missed the updates. The administrator can manually initiate the updates from the 'AV Scan' interface.

### To manually update the virus signature database on selected devices

- Click the 'Inventory' tab from the left hand side and choose 'Antivirus'.
- If you want update the virus database only on specific devices, select the devices. If you want to run the update the database on all the devices, you need not select the devices.



- If you want to update the database on selected devices, click the 'Update AV DB for selected' button. If you want to update the database on all the devices at-once, click the 'Update AV DB for all' button.



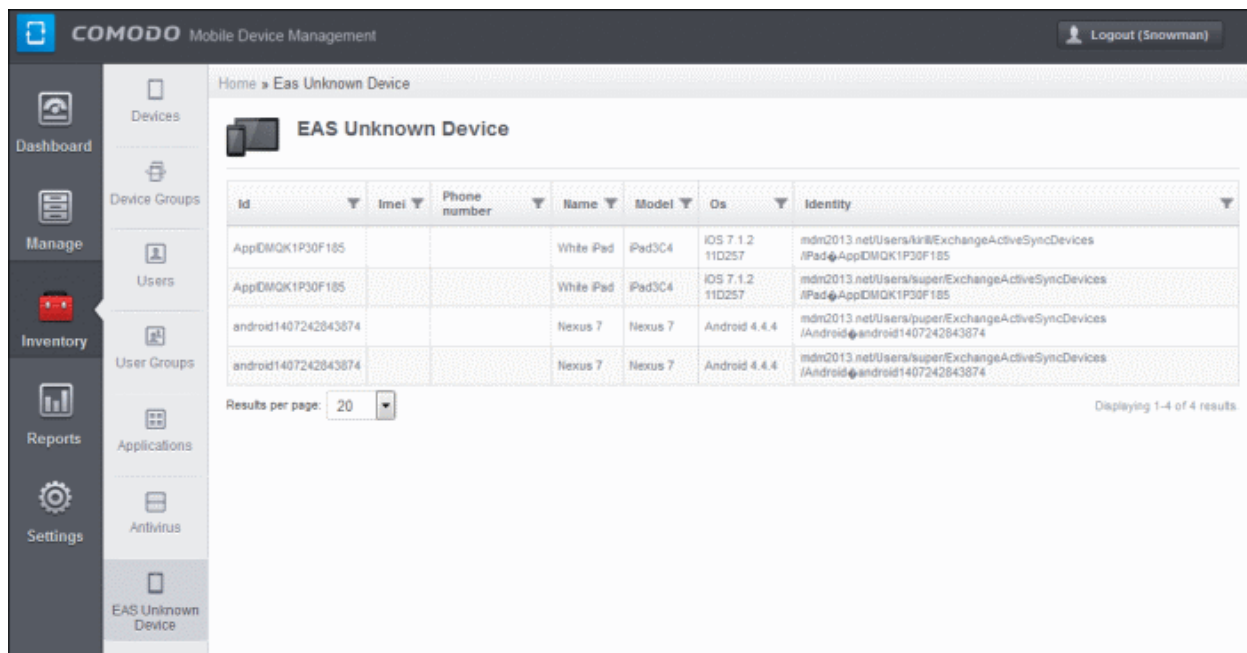
## 5.7.EAS Unknown Devices

CMDM is capable of connecting mobile devices to Exchange server and allow users access to company emails from their devices. The enrolled mobile devices in CMDM can be connected to the Exchange server after installing Comodo's MDM Exchange Service on the same machine where the Exchange server is installed. MDM Exchange service utilizes the Exchange ActiveSync (EAS) protocol for connecting to CMDM. Refer to the section **Installing Exchange Service** for more details.

In order to guarantee a secure connection after Exchange Service installation is complete, all new devices and devices whose IMEI haven't been defined are sent to the Quarantine Mode by default. After checking devices' IMEI in the quarantine list with that of the devices enrolled, CMDM assigns a new rule as 'Allow' for iOS devices automatically. For Android devices in the quarantine list, the administrator has to associate them manually with that available in the Devices screen. Refer to the sections **Managing an Individual Device** and **Associating EAS Unknown Devices** for more details.

- Click the Inventory tab from the left hand side navigation and choose 'EAS Unknown Device' from the options.

The EAS Unknown Device screen displays the list of unknown devices that are quarantined.



EAS Unknown Devices – Column Description	
Column Heading	Description
ID	The unique number assigned to the device.
IMEI	The International Mobile Equipment Identity (IMEI) number of the device.
Phone Number	Displays the phone number of the user.
Name	The name assigned to the device by the user. If no name is assigned, the model number of the device will be used as the name of the device.
Model	Indicates the model number of the device.
OS	Displays the OS type which the device supports.
Identity	Indicates the identity data assigned to the device.

### Sorting, Search and Filter Options

- Clicking a funnel  button beside a column header to display the sorting and filtering options.

**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

Contains

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## 6. Reports

CMDM Reports are highly informative summaries of the security and status of enrolled devices. The reports contain details of compliance status of devices, about viruses found in scanned devices, logs of devices, logs of user activity and push statistics reports.

Home » Threats report

**Threat Report**  
The list of viruses that are not processed.

The list of viruses that are not processed:

Signature ID	Signature name	Package name	Date time	Device name	Device type	Device platform	Last Scanned	Last Activity	Owner
6761	Android.PJA-High-AirPush.D	com.superromanticlive.wallpaper.droidapp	2014/09/02 12:22:20 PM	Setty Ericason_WT191	Smartphone	Android	2014/09/02 12:22:20 PM	2014/09/02 12:22:20 PM	Snowman

Results per page: 20

Displaying 1-1 of 1 result.

Click the following links for detailed explanations on each of the reports.

- [Threat Reports](#)
- [Event Logs from Individual Devices](#)
- [User Activity Logs](#)



## 6.1. Viewing Threats Reports


The Threats reports interface provides administrators a summary of viruses found on devices that are not processed. Refer to the section [Managing Antivirus and Running Scans on Enrolled Devices](#) and [Profiles for Android Devices](#) for more details on running on demand and scheduling antivirus scans respectively.

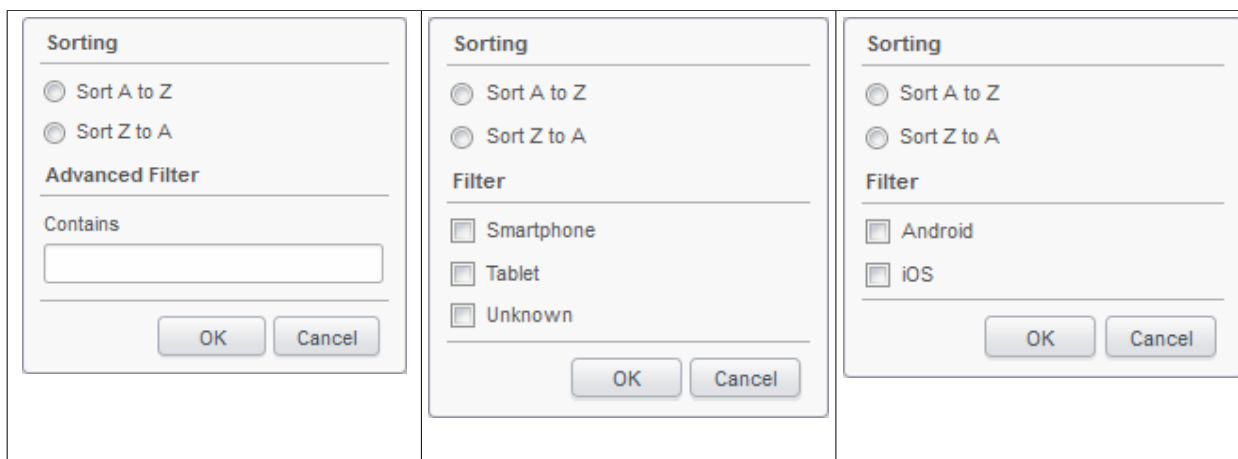
To view the threat reports, click 'Reports' in the left side navigation and then 'Threats Report'.

**Threats Report - Column Descriptions**

Column Heading	Description
Signature ID	The unique ID of the virus signature.
Signature name	The name of the virus signature as in blacklist of CMDM.
Package name	Indicates the identifier of the app which infected the device.
Date time	Indicates the date and time when the virus was detected.
Device name	The name of the device on which the virus was found.
Device Type	Displays whether the device is a smartphone or a tablet.
Device platform	Displays the operating system of the infected device.
Last Scanned	Indicates the date and time of the last antivirus scan.
Last Activity	Displays the date and time of device connected to CMDM last.
Owner	Displays the username of the device enrolled in CMDM.

### Sorting, Search and Filter Options

- Click a funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



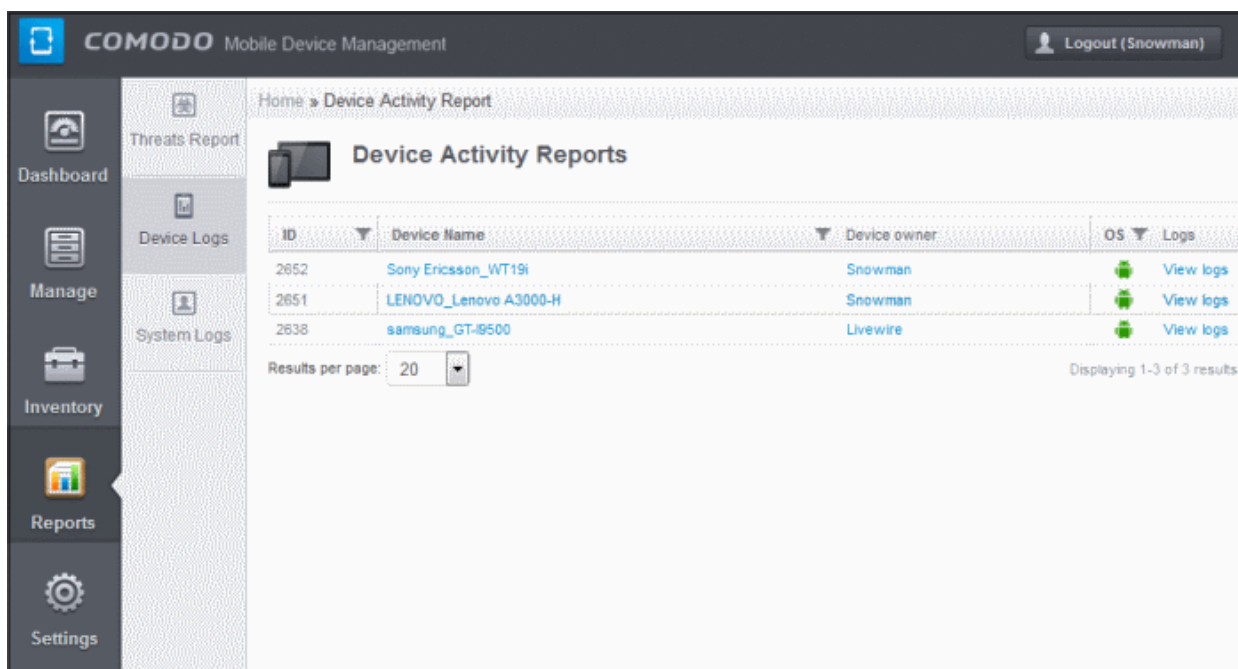
- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## 6.2. Viewing Event Logs from Individual Devices

The Devices Activities Report provides activity logs of all the enrolled devices in CMDM. The log report of devices include system generated activities such as virus alerts, info regarding location and administrator actions such as virus scan command and more.


To view the Devices Activities report, click 'Reports' in the left side navigation and then 'Devices Logs'.

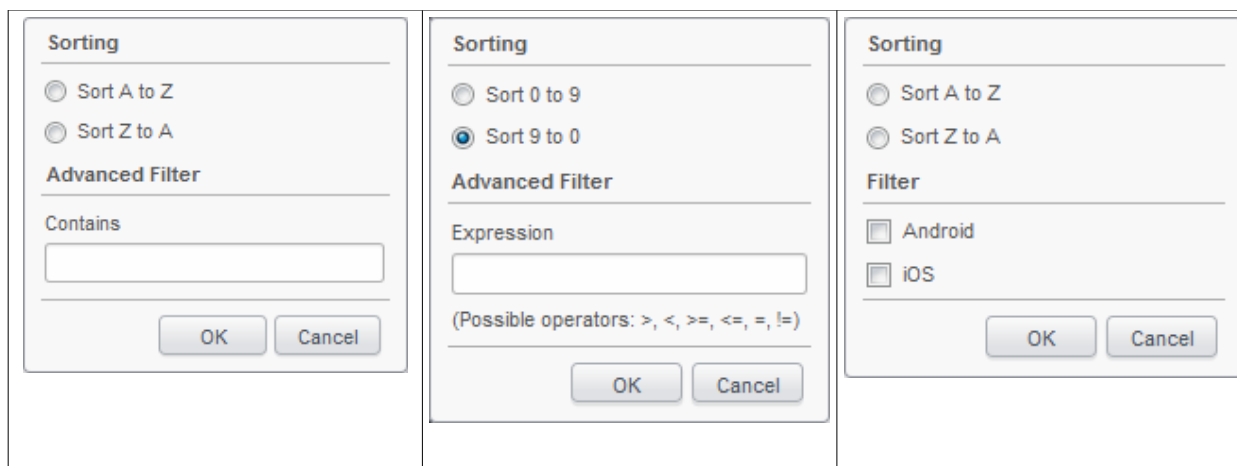
The Devices Activities report screen will be displayed:



Devices Activities Report - Column Descriptions	
Column Heading	Description
ID	The unique ID of the report for a device.
Device Name	Name of the device. Clicking on the name link will display the full details of the device. Refer to the section ' <a href="#">Managing an Individual Device</a> ' for more details.
Device owner	Displays the username of the device enrolled in CMDM. Clicking on the username link will display the details of the user. Refer to the section ' <a href="#">Viewing the Details of a User</a> ' for more details.
OS	Displays the operating system of the device.
View Logs	Clicking on the 'View Logs' link will display the detailed log for the device since it was enrolled in CMDM. Refer to the section ' <a href="#">Viewing Log of a Device</a> ' for more details.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## Viewing Log of a Device

The Action Log of a device provides full details of all the CMDM related activities taken place in the device. The activities includes system generated as well as admin generated actions. To view the logs of a device, click 'Report' in the left side navigation, then 'Devices Logs'. In the 'Devices Activities Report' page, click the 'View logs' link at the far end in the row of the device that you would like to view the log.

Home » Device Activity Report

## Device Activity Reports

ID	Device Name	Device owner	OS	Logs
2582	iPhone 4s(Comodo)	stepan		<a href="#">View logs</a>
2581	ZTE_Blade S	greg		<a href="#">View logs</a>
2578	HUAWEI_HUAWEI-U8850	stepan		<a href="#">View logs</a>
2546	asus_Nexus 7	morten_ha		<a href="#">View logs</a>
2528	LENOVO_Lenovo A850	greg		<a href="#">View logs</a>
2496	LGE_LG-P715	sergey		<a href="#">View logs</a>

Results per page:

Displaying 1-6 of 6 results.

The detailed log page for the selected device will be displayed:

Home » Device Activity Report » iPhone 4s iOS7.1

## Device Logs: iPhone 4s iOS7.1

ID	Type	Log time	Username	Description
91620	Info	2014/08/18 01:14:40 PM	[system]	Request sent install application [id:320 name:CMDM].
91613	Info	2014/08/18 01:05:30 PM	[system]	Update device information.
91605	Info	2014/08/18 01:04:42 PM	[system]	Got location [latitude: 46.464971, longitude: 30.720173, accuracy: 65] from device [iPhone 4s iOS7.1].
91582	Info	2014/08/18 12:45:30 PM	[system]	Update device information.
91577	Info	2014/08/18 12:44:43 PM	[system]	Got location [latitude: 46.464897, longitude: 30.720069, accuracy: 65] from device [iPhone 4s iOS7.1].
91559	Info	2014/08/18 12:25:30 PM	[system]	Update device information.
91558	Info	2014/08/18 12:24:42 PM	[system]	Got location [latitude: 46.464986, longitude: 30.720141, accuracy: 65] from device [iPhone 4s iOS7.1].
91530	Info	2014/08/18 12:05:30 PM	[system]	Update device information.
91525	Info	2014/08/18 12:04:43 PM	[system]	Got location [latitude: 46.464963, longitude: 30.720154, accuracy: 65] from device [iPhone 4s iOS7.1].
91486	Info	2014/08/18 11:45:30 AM	[system]	Update device information.
91485	Info	2014/08/18 11:44:43 AM	[system]	Got location [latitude: 46.464967, longitude: 30.720151, accuracy: 65] from device [iPhone 4s iOS7.1].
91468	Info	2014/08/18 11:25:30 AM	[system]	Update device information.
91466	Info	2014/08/18 11:24:52 AM	[system]	Got location [latitude: 46.464939, longitude: 30.720172, accuracy: 65] from device [iPhone 4s iOS7.1].
91465	Info	2014/08/18 11:24:49 AM	[system]	Update device information.
91455	Info	2014/08/18 11:16:17 AM	stepan	Send Message [ghihjtyf] to device [iPhone 4s iOS7.1].
91451	Info	2014/08/18 11:10:46 AM	stepan	Request sent update device information.
91447	Info	2014/08/18 11:05:15 AM	stepan	Request sent update device information.
91312	Info	2014/08/17 02:25:58 PM	[system]	Update device information.
91310	Info	2014/08/17 02:24:44 PM	[system]	Got location [latitude: 46.464966, longitude: 30.720153, accuracy: 65] from device [iPhone 4s iOS7.1].
91305	Info	2014/08/17 02:05:31 PM	[system]	Update device information.

Go to page:

Results per page:


Displaying 1-20 of 299 results.

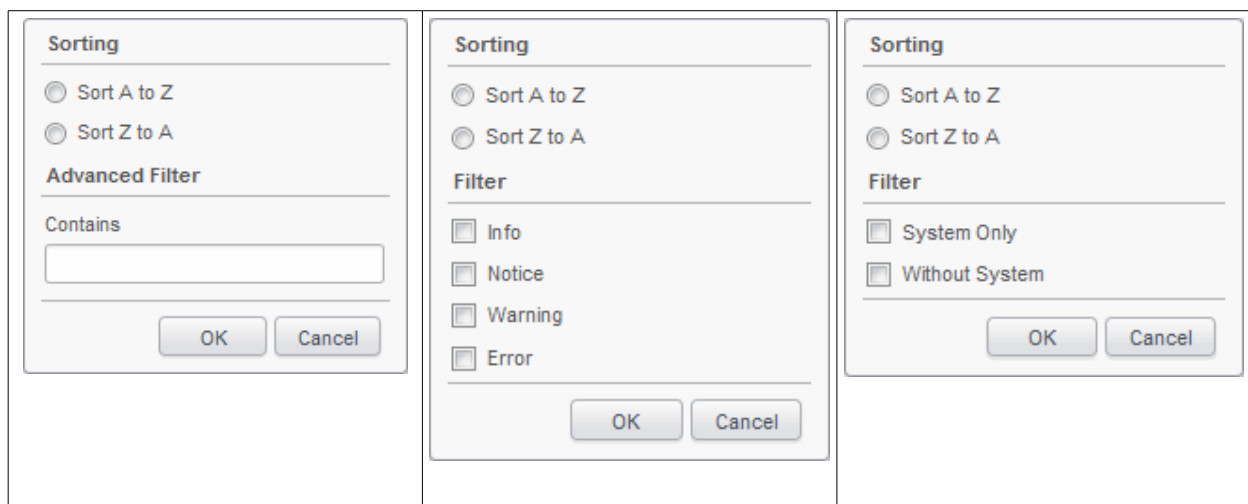
### Device Log Report - Column Descriptions

Column Heading	Description
ID	The unique ID of the log for a device.

Type	Indicates the type of activity that was recorded for the device. For example, a virus scan command from an administrator will be recorded as Notice, system generated activity such as location detection will be recorded as Info and virus detected by CMDM will be recorded as Warning.
Log time	Displays the date and time of the activity recorded.
Username	Displays the details whether it was system generated activity or the name of the administrator who initiated the action. Clicking on the username link will display the details of the user. Refer to the section <b>'Viewing the Details of a User'</b> for more details.
Description	Displays the details of the activity that was recorded.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## 6.3. Viewing User Activity Logs

CMDM keeps track of activities initiated by the system, administrators as well as by users. The activities recorded include logins, logouts, send virus scan commands, send shutdown command to devices and more. To view report of user activity, click the 'View logs' link at the far end in the row of the user that you would like to view the log. The log is very useful to know who did what at a later stage. Please note the 'User Logs' will not be available for system generated events.


To view the User Activity Report, click 'Reports' in the left side navigation and then 'System Logs'.

The 'User Activity Report' will be displayed.

ID	Type	Log time	Username	Description	User Log
92399	Info	2014/08/18 07:25:32 PM	[system]	Update device information.	
92398	Info	2014/08/18 07:25:32 PM	[system]	Got location [latitude: 46.464997, longitude: 30.720170, accuracy: 30] from device [ZTE_Blade S].	
92397	Info	2014/08/18 07:25:31 PM	[system]	Update device information.	
92395	Notice	2014/08/18 07:24:21 PM	greg	Update profile [iOs Test].	User Logs
92395	Notice	2014/08/18 07:23:58 PM	greg	Update profile [iOs Test].	User Logs
92394	Info	2014/08/18 07:23:52 PM	[system]	Update device information.	
92393	Info	2014/08/18 07:23:38 PM	[system]	Got location [latitude: 46.464999, longitude: 30.720225, accuracy: 20] from device [HUAWEI_HUAWEI-U0850].	
92392	Info	2014/08/18 07:23:34 PM	[system]	Got location [latitude: 46.465135, longitude: 30.719988, accuracy: 65] from device [iPhone 4s(Comodo)].	
92391	Notice	2014/08/18 07:23:20 PM	greg	Update profile [iOs Test].	User Logs
92390	Info	2014/08/18 07:20:22 PM	[system]	Update device information.	
92389	Info	2014/08/18 07:20:22 PM	[system]	Got location [latitude: 46.465009, longitude: 30.720235, accuracy: 20] from device [ZTE_Blade S].	
92388	Notice	2014/08/18 07:20:18 PM	greg	Update profile [test iOs].	User Logs
92387	Info	2014/08/18 07:18:40 PM	[system]	Update device information.	

User Activity Report - Column Descriptions	
Column Heading	Description
ID	The unique ID of the report log.
Type	Indicates the type of activity that was recorded for the user. For example, a virus scan command from an administrator will be recorded as Notice, send lock and unlock commands as warning, logins and logouts as info.
Log time	Displays the date and time of the activity recorded.
Username	Displays login name of the users and administrators who initiated the action. Clicking on the username link will display the details of the user. Refer to the section <b>'Viewing the Details of a User'</b> for more details.
Description	Displays the details of the activity that was recorded.
User Logs	Clicking on the 'View User Logs' link will display the detailed log for the user activity. Refer to the section <b>'Viewing Log of a User'</b> for more details.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options. Some examples are shown below:

**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

Contains

**Sorting**

Sort A to Z

Sort Z to A

**Filter**

Info

Notice

Warning

Error



- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## Viewing Log of a User

In the 'User Activity Report' page, click the 'User Logs' link at the far end in the row of the user that you would like to view the log.

Home » User activity report

### User Activity Report

User activity report

ID	Type	Log time	Username	Description	User Log
91640	Info	2014/05/18 01:21:59 PM	[system]	Update device information.	
91639	Info	2014/05/18 01:20:45 PM	[system]	Update device information.	
91638	Info	2014/05/18 01:20:43 PM	[system]	Got location [latitude: 13.030126, longitude: 80.237671, accuracy: 243] from device [Sony Ericsson_WT19].	
91637	Info	2014/05/18 01:20:42 PM	[system]	Update device information.	
91636	Info	2014/05/18 01:20:42 PM	[system]	Got location [latitude: 46.465013, longitude: 30.720157, accuracy: 30] from device [ZTE_Blade S].	
91635	Info	2014/05/18 01:20:05 PM	[system]	Got location [latitude: 46.464992, longitude: 30.720212, accuracy: 20] from device [ZTE_Blade S].	
91634	Info	2014/05/18 01:20:04 PM	[system]	Got location [latitude: 46.465002, longitude: 30.720222, accuracy: 20] from device [ZTE_Blade S].	
91633	Info	2014/05/18 01:17:50 PM	[system]	Request sent install application [id:320 name:CMDM].	
91632	Info	2014/05/18 01:16:32 PM	[system]	Request sent install application [id:320 name:CMDM].	
91631	Info	2014/05/18 01:16:32 PM	[system]	Request sent install application [id:314 name:Gismeteo lite].	
91630	Info	2014/05/18 01:16:31 PM	[system]	Request sent install application [id:320 name:CMDM].	
91629	Info	2014/05/18 01:16:31 PM	[system]	Request sent install application [id:314 name:Gismeteo lite].	
91628	Info	2014/05/18 01:16:31 PM	[system]	Update device information.	
91627	Info	2014/05/18 01:15:36 PM	[system]	Update device information.	
91626	Info	2014/05/18 01:15:35 PM	[system]	Got location [latitude: 46.465007, longitude: 30.720217, accuracy: 20] from device [ZTE_Blade S].	
91625	Info	2014/05/18 01:15:35 PM	admin	Login.	User Logs
91624	Info	2014/05/18 01:15:34 PM	[system]	Update device information.	
91623	Info	2014/05/18 01:15:33 PM	[system]	Got location [latitude: 13.030126, longitude: 80.237671, accuracy: 243] from device [Sony Ericsson_WT19].	
91622	Warning	2014/05/18 01:15:11 PM	[system]	Delete device [Phone 4s(Comodo)] confirmation.	
91621	Info	2014/05/18 01:14:40 PM	[system]	Request sent install application [id:320 name:CMDM].	

Go to page: 1 2 3 4 5 6 7 8 9 10 Next > Last >>

Results per page: 20

Displaying 1-20 of 91640 results.

The detailed log page for the selected user or administrator will be displayed:



Home » Activity report by user: admin

## Activity Report: admin

ID	Type	Log time	Description
91625	Info	2014/08/18 01:15:35 PM	Login.
89493	Info	2014/08/15 05:56:28 PM	Login.
89167	Info	2014/08/15 02:38:16 PM	Send location request command to device [iPhone 4s(Comodo)].
89164	Info	2014/08/15 02:37:57 PM	Send location request command to device [iPhone 4s(Comodo)].
89163	Info	2014/08/15 02:37:37 PM	Login.
84653	Info	2014/08/12 04:05:19 PM	Login.
84503	Info	2014/08/11 04:25:34 PM	Login.
83530	Info	2014/08/04 05:30:30 PM	Login.
74845	Info	2014/07/21 01:32:43 PM	Login.
63346	Notice	2014/05/27 02:16:13 PM	Update user data [aUsername].
43279	Info	2014/05/22 04:46:57 PM	Login.
43073	Info	2014/05/22 12:17:12 PM	Login.
22194	Info	2014/03/13 08:36:24 PM	Login.
21636	Info	2014/03/13 06:35:43 PM	Login.
19539	Info	2014/02/27 06:45:47 PM	Login.
19223	Info	2014/02/12 05:41:17 PM	Login.
15888	Info	2013/12/20 02:41:02 PM	Send location request command to device [samsung_GT-I9500].
15887	Info	2013/12/20 02:40:49 PM	Login.
6174	Warning	2013/11/05 12:34:57 PM	Send lock UNLOCK command to device [Genymotion_Nexus One - 4.2.2 - with Google Apps - API 17 - 480x800].
6173	Warning	2013/11/05 12:34:52 PM	Send lock LOCK with Password: 111 command to device [Genymotion_Nexus One - 4.2.2 - with Google Apps - API 17 - 480x800].

Go to page: 1 2 Next > Last >> Displaying 1-20 of 34 results.

Results per page: 20

Activity Report by User - Column Descriptions	
Column Heading	Description
ID	The unique ID of the report log.
Type	Indicates the type of activity that was recorded for the user. For example, a virus scan command will be recorded as Notice, login and logout as Info and send lock command as Warning.
LogTime	Displays the date and time of the activity recorded.
Description	Displays the details of the activity that was recorded.

### Sorting, Search and Filter Options

- Click the funnel button beside a column header to display the sorting and filtering options. Some examples are shown below:

The image displays two side-by-side screenshots of the Comodo Mobile Device Manager interface. The left screenshot shows a 'Sorting' dialog box with two radio button options: 'Sort 0 to 9' (unselected) and 'Sort 9 to 0' (selected). Below this is an 'Advanced Filter' section with a text input field labeled 'Expression' and a note '(Possible operators: >, <, >=, <=, =, !=)'. At the bottom are 'OK' and 'Cancel' buttons. The right screenshot shows a 'Filter' dialog box with two radio button options: 'Sort A to Z' (selected) and 'Sort Z to A' (unselected). Below this is a 'Filter' section with four checkboxes: 'Info', 'Notice', 'Warning', and 'Error', all of which are currently unchecked. At the bottom are 'OK' and 'Cancel' buttons.

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter / select the required search item(s) and click 'OK'.
- To display all the items again, remove / deselect the search key from filter and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

## 7. Configuring Comodo Mobile Device Manager

The 'Settings' tab enables administrators to create admin and user roles with different privilege levels, assign appropriate roles to enrolled users and configure the behavior of various CMDM components. This tab also allows administrators to manage subscriptions and renew/upgrade licenses as well as configure Google Cloud Messaging (GCM) token and add Apple Push Notification (APN) certificate.

Home » Subscription and License

### License Details

208a4955-af4b-48f1-aa31-d843683794 (support)  
Will expire in 149 day(s)

Subscription ID	880e1310df
License key	208a4955-af4b-48f1-aa31-d843683794
Max. Users	99
Organization	
Licensed to	
Free	No
Active	Yes
Valid From	2014-01-30T13:26:29+04:00
Expires	2015-01-30T13:26:29+04:00
Time check	2014-09-02T13:08:00+04:00
License Registered at	2014-03-13T15:51:31+04:00

Copyright © 2014 Comodo (v 2.5.557.1275)


The following sections provide detailed explanations on configuring various features and settings.

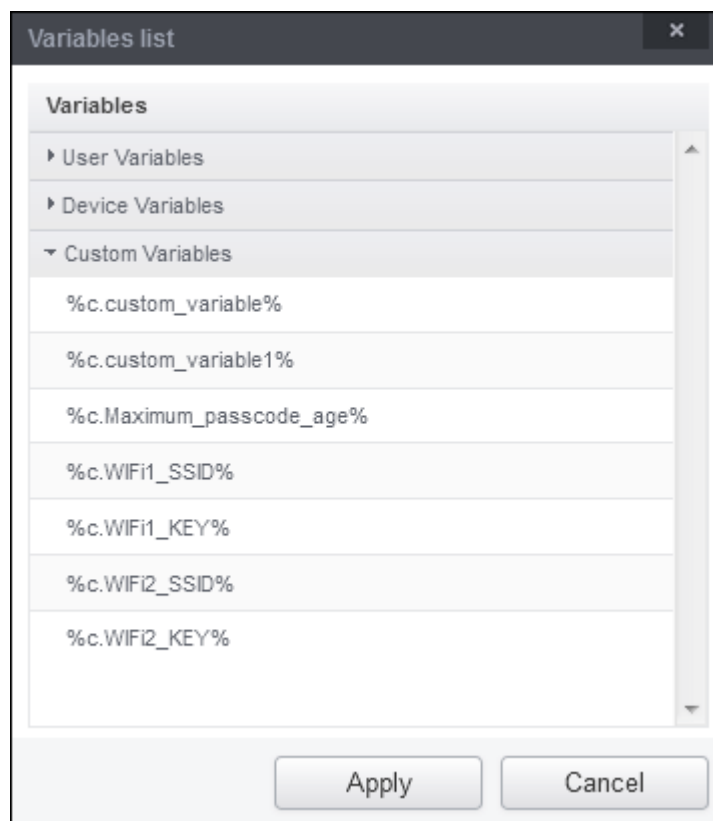
- **Configuring Custom Variables**
- **Configuring Email Templates**
- **Adding Apple Push Notification Certificate**
- **Configuring Google Cloud Messaging (GCM) for Android**
- **Configuring the Android Agent**
- **Configuring the Role-Based Access Control for Users**
  - **Creating a New Role**
  - **Managing Permissions and Assigned Users of a Role**
  - **Removing a Role**
  - **Managing Roles assigned to a User**
- **Importing User Groups from LDAP**

- [Antivirus Settings](#)
- [Viewing and Managing Removed Devices](#)
- [Viewing and Managing Licenses](#)
- [Generating MDM Exchange Service Token](#)
- [Viewing Version Information](#)

## 7.1. Configuring Custom Variables

CMDM is capable of fetching values from variables. There are three types of variables available in CMDM, User Variables, Device Variables and Custom Variables, that can be used by the administrator for fetching the values. The 'Variable list' screen

will appear when the 'Insert Variable' button  is clicked. This button is available in several interfaces for the purpose of inserting variables in the Profiles section. The first two, User Variables and Device Variables are hard coded and cannot be altered. These are useful for fetching the values of user and devices, for example user login details, email details from Inventory > Users and Devices. The last one, Custom Variables, can be created by the administrators and the variables created will be shown below the first two.




The custom variables can be added in Settings > Custom Variables. These are useful for rolling changes across all profiles that have custom variables inserted. For example, if an administrator has provided a variable for an app in the AV scanning exclusion list in the Anti-virus settings of a profile and wants to change the app, he can just change the value in the custom variable screen. The changes will be rolled out to all profiles that has this custom variable.

To access the Custom Variable screen, click 'Settings' in the left side navigation and then 'Custom Variables'.

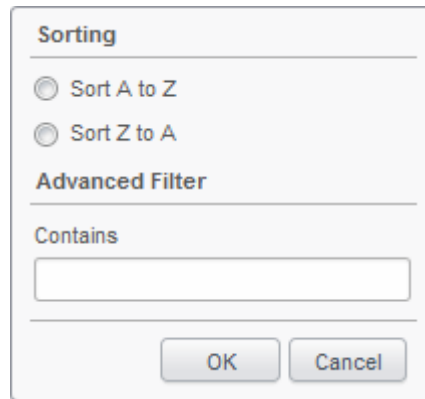
The screenshot shows the 'Custom Variables' page in the Comodo Mobile Device Management interface. The page title is 'Home > Custom Variables'. Below the title, there is a sub-header 'Custom Variables' and 'Variable system'. The main content is a table with the following columns: Key, Value, Creator, Time creation, Last modified, and Time last modified. There are 6 rows of data, each with a red 'X' icon in the controls column. Below the table, there is a 'Results per page' dropdown set to 20, a 'Displaying 1-6 of 6 results' message, and a 'Create new Variable' button.

Key	Value	Creator	Time creation	Last modified	Time last modified	Controls
%c.WF2_SSD%	CIS_DEV	Livewire	2014/08/21 11:45:18 AM			X
%c.WF2_KEY%	mianBaN72yeDeVLP	Livewire	2014/08/21 11:45:56 AM			X
%c.WF1_SSD%	CMDM	Livewire	2014/08/21 11:44:19 AM			X
%c.WF1_KEY%	QwaS12ZX!	Livewire	2014/08/21 11:44:50 AM			X
%c.Maximum_passcode_age%	Passcode Age	Snowman	2014/08/18 12:29:19 PM			X
%c.custom_variable1%	Look my secret custom variable1	Ironhorse	2014/08/12 04:52:27 PM			X

Custom Variables - Column Descriptions	
Column Heading	Description
Key	Displays the name of key for the value in the next column. Clicking the key will open the 'Edit Variable' interface that allows to edit the value for the key. Please note the key name cannot be edited.
Value	Displays the value for the key in the preceding column.
Creator	Displays the name of administrator that has created the custom variables. Clicking the name of the administrator will open the 'View User' pane, displaying the details of the user. Refer to the section <b>Viewing the details of the User</b> for more details.
Time Creation	Displays the custom variable created date and time.
Last modified	Displays the name of the user that last modified the custom variable.
Time last modified	Indicates the date and time when the variables was edited.
Controls	 Enables the administrator to remove custom variables.

## Sorting, Search and Filter Options

- Click the funnel  button beside a column header to display the sorting and filtering options.



**Sorting**

Sort A to Z

Sort Z to A

**Advanced Filter**

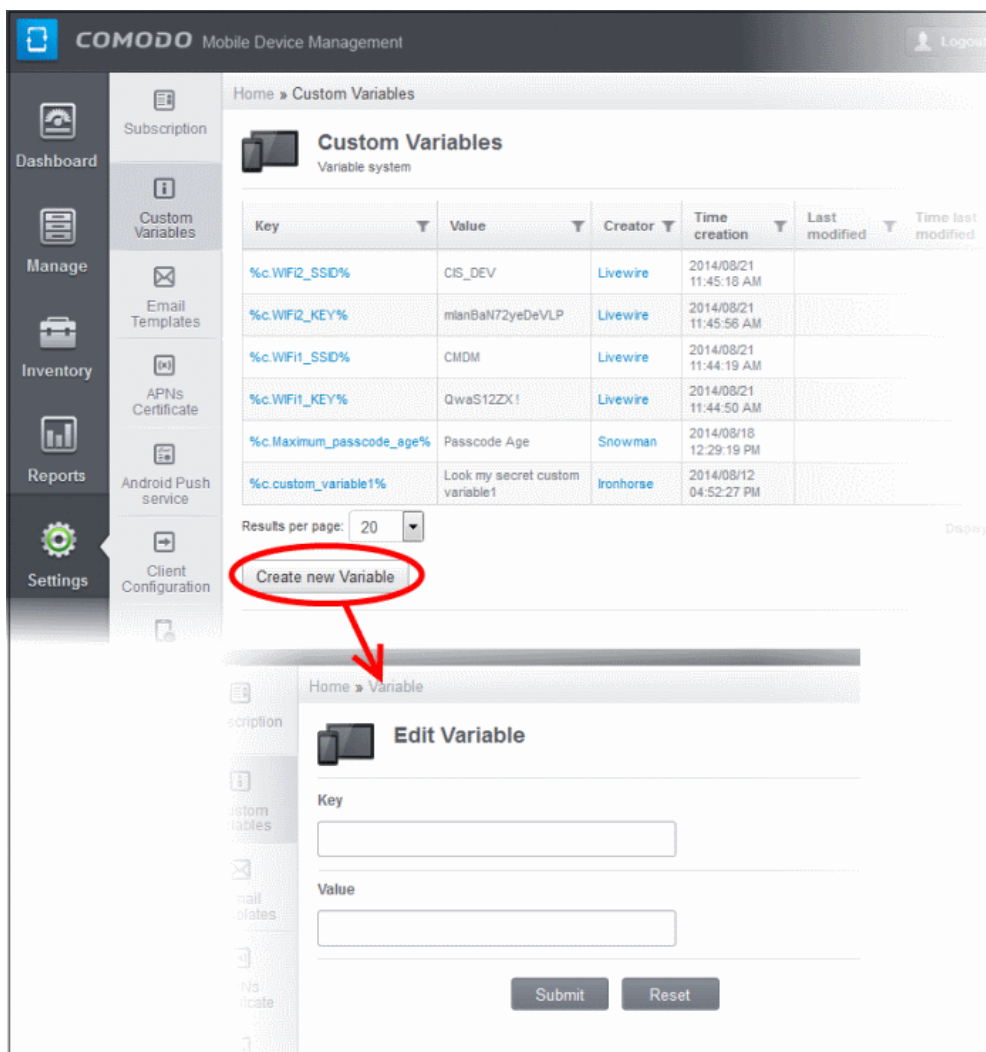
Contains

OK Cancel

- To sort the items, select the required option and click 'OK'.
- To filter the items based on search criteria, enter a search key word partially or fully in the text field under Advanced Filter and click 'OK'.
- To display all the items again, remove the search key from the text field and click 'OK'.
- By default CMDM returns 20 results per page when you perform a search. To increase the number of results displayed per page up to 200, click the arrow next to 'Results per page' drop-down.

#### To create a new Custom Variable

- Click the 'Settings' tab from the left and choose 'Custom Variables'
- Next, click 'Create new Variable' at the bottom of the 'Custom Variables' interface:



- In the 'Edit Variable' interface type a variable name in the 'Key' text box.
- In the 'Value' text field, enter the value for the variable.
- Click 'Reset' to clear the fields.
- Click 'Submit' to add the variable to CMDM.

The variable will be added and displayed in the list.

### To edit a Custom Variable

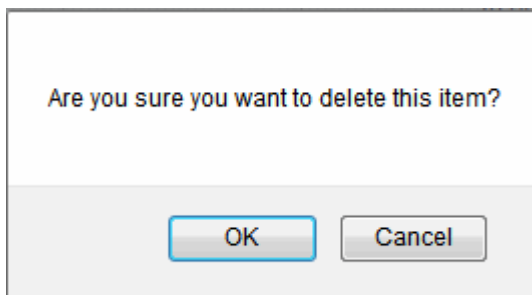
- Click the 'Settings' tab from the left and choose 'Custom Variables'
- Click on the name of the Custom Variable to be edited.
- In the Edit Variable screen, edit the values and click the Submit button.

### To remove a Custom Variable

- Click the 'Delete' icon  at the far end the row of the variable that you want to remove.

A confirmation dialog will appear.





- Click 'OK' to remove the variable. The Custom Variable will be removed from the list.


## 7.2. Configuring Email Templates

CMDM allows administrators to customize the notification emails sent to users. There are six types of notification emails and these can be customized according to the organizational requirements. The administrators can edit the email subject and content and insert appropriate variables. For each type of email template, appropriate variables will be available in the toolbar. Make sure not to change the variable name as these will not work at all or fetch wrong values.

To access the Email Templates screen, click 'Settings' in the left side navigation and then 'Email Templates'.


Name	E-mail subject	Content
Activate account	Comodo Mobile Device Manager - Account activation	%username% - Name of registered user %activateLink% - Link for Activate and set password
Password reset	Comodo Mobile Device Manager - Password Reset Confirmation	%username% - Name of registered user %linkResetPass% - Link for reset password %supportEmail% - Support email %currentDate% - Current date
Device enrollment	Comodo Mobile Device Manager - Device Enrollment	%profileLink% - Link on profile %downloadLink% - Link for download %settingLink% - Link for settings %hostWithoutPort% - Hostname without port %serverPort% - Server port %token% - Token or pin code
Device enrollment over LDAP	Comodo Mobile Device Manager - Device Enrollment	%adLink% - Active Directory credentials %downloadLink% - Link for download %settingLink% - Link for settings %hostWithoutPort% - Hostname without port %serverPort% - Server port
Enrollment email for servers with self signed SSL certificates	Comodo Mobile Device Manager - Device Enrollment	%selfSignedLink% - Self signed certificate link %profileLink% - Link on profile %downloadLink% - Link for download %settingLink% - Link for settings %hostWithoutPort% - Hostname without port %serverPort% - Server port %token% - Token or pin code
Enrollment email for servers with self signed SSL certificates over LDAP	Comodo Mobile Device Manager - Device Enrollment	%selfSignedLink% - Self signed certificate link %adLink% - Active Directory credentials %downloadLink% - Link for download %settingLink% - Link for settings %hostWithoutPort% - Hostname without port %serverPort% - Server port

Results per page: 20 | Displaying 1-6 of 6 results

Email Templates- Column Descriptions	
Column Heading	Description
Name	Indicates the name of email template. This cannot be edited.
E-mail subject	Displays the details of the email subject.
Content	Displays the variable name and its value. This cannot be edited.
Controls	 Allows administrators to edit the email template.

- By default CMDM displays 20 entries per page. To increase the number of entries displayed per page up to 200, click the arrow next to 'Results per page' drop-down.


### To edit an email template

- Click the 'Settings' tab from the left and choose 'Email Templates'
- Click the  icon at the far end of the row of the email template that you want to edit.

The template editor of the respective Email type will be displayed. For example, if you click the edit icon beside the 'Account activation' email template, the following template editor will be displayed.

Home » Email Templates » Edit template - Comodo Mobile Device Manager - Account activation

---




## Comodo Mobile Device Manager - Account activation

Email Templates

---

**E-mail subject**

Comodo Mobile Device Manager - Account activation



Dear %username%,

Congratulations, your Comodo Mobile Device Manager account has been successfully created. Please click the following link to activate your account and set up your password:

[%activateLink%](#)

Sincerely,  
Comodo Mobile Device Management team

Editor
Source

Submit

Cancel

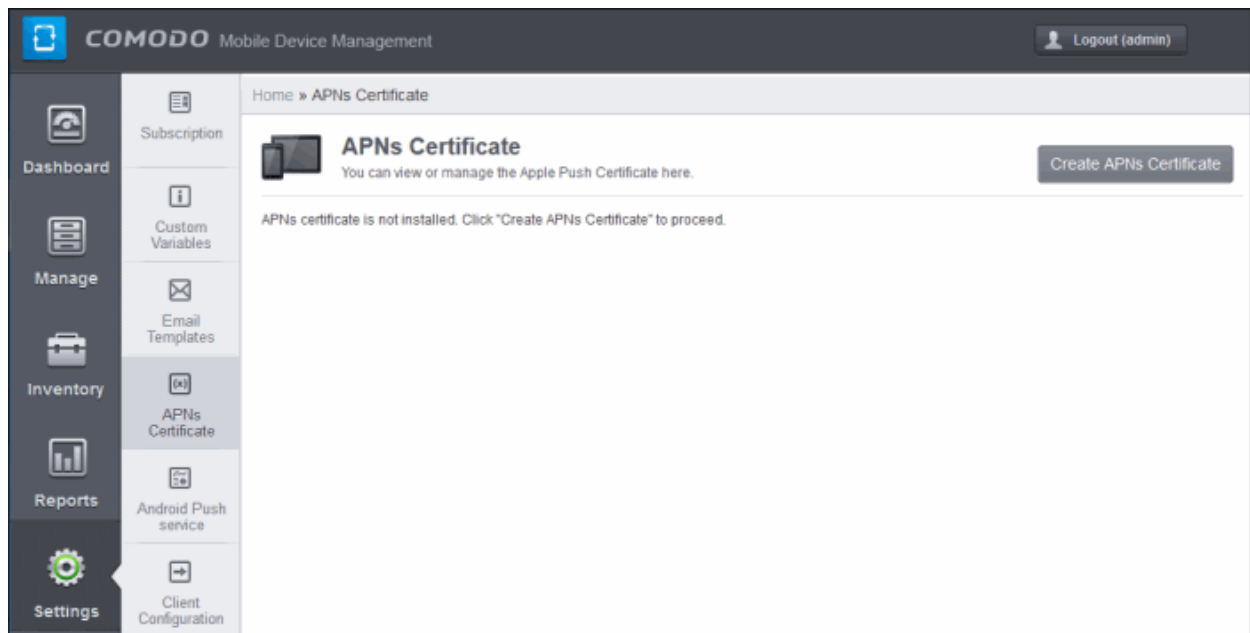
- Edit the email template per your requirements and insert the variables available in the toolbar wherever required.
- Click the 'Submit' button to save the changes.

## 7.3. Adding Apple Push Notification Certificate

In order to communicate with iOS devices, Apple requires that you obtain an Apple Push Notification (APNs) certificate and corresponding private key. Please follow the steps below to apply for and implement an APN certificate:

### Step 1– Generate your PLIST

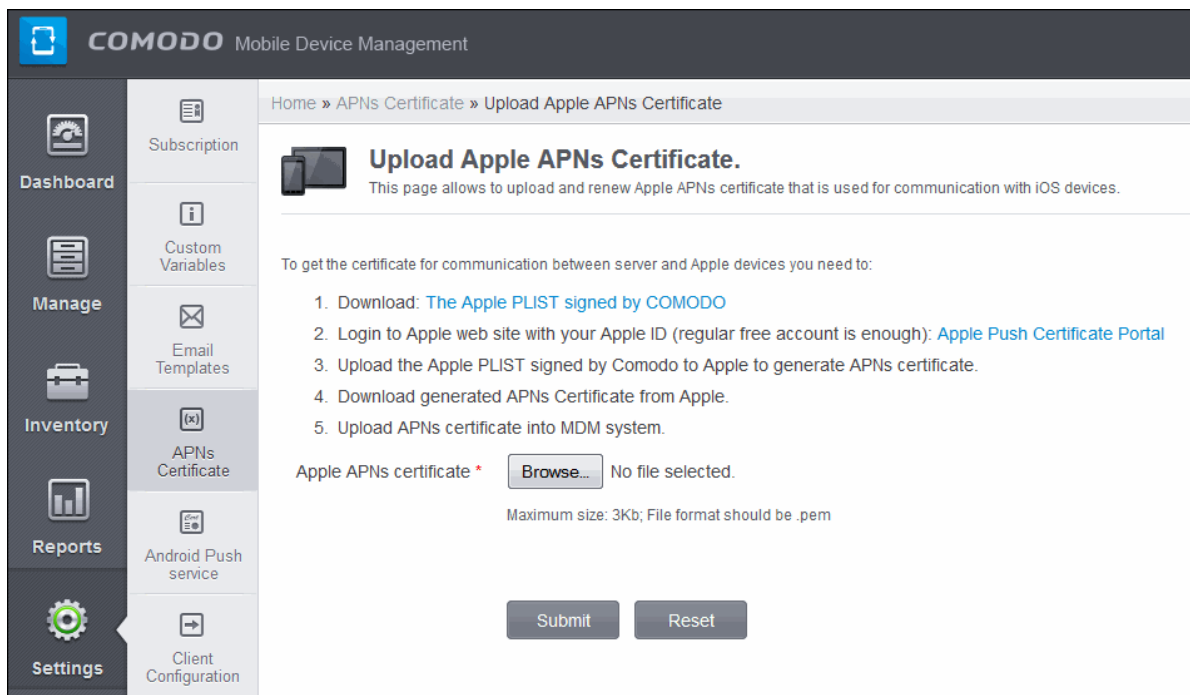
- In the CMDM interface, click 'Settings' followed by 'APNs Certificate' on the left.



- Click the 'Create APNs Certificate' button at the top-right to open the APN certificate application form. The fields on this form are for a Certificate Signing Request (CSR):

- Complete all fields marked with an asterisk and click 'Submit'. This will send a request to Comodo to sign the CSR and generate an Apple PLIST. You will need to submit this to Apple in order to obtain your APN certificate. Usually your

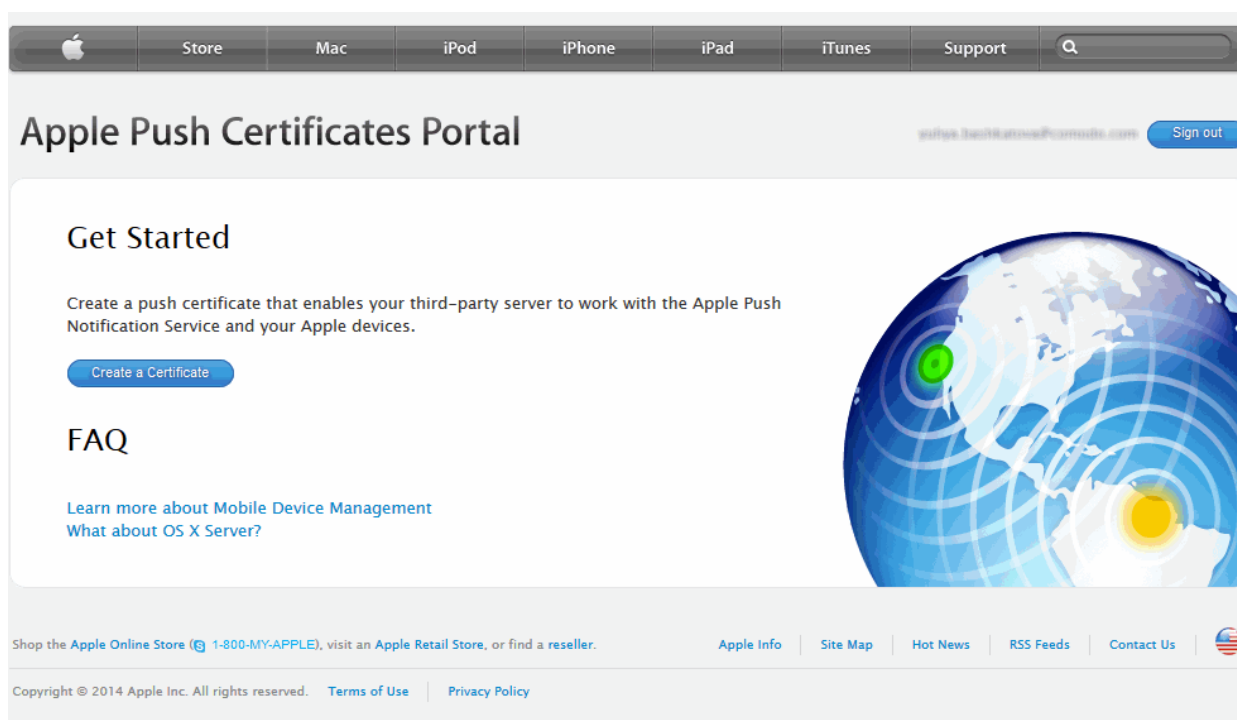
request will be fulfilled within seconds and you will be taken to a page which allows you to download the PLIST:



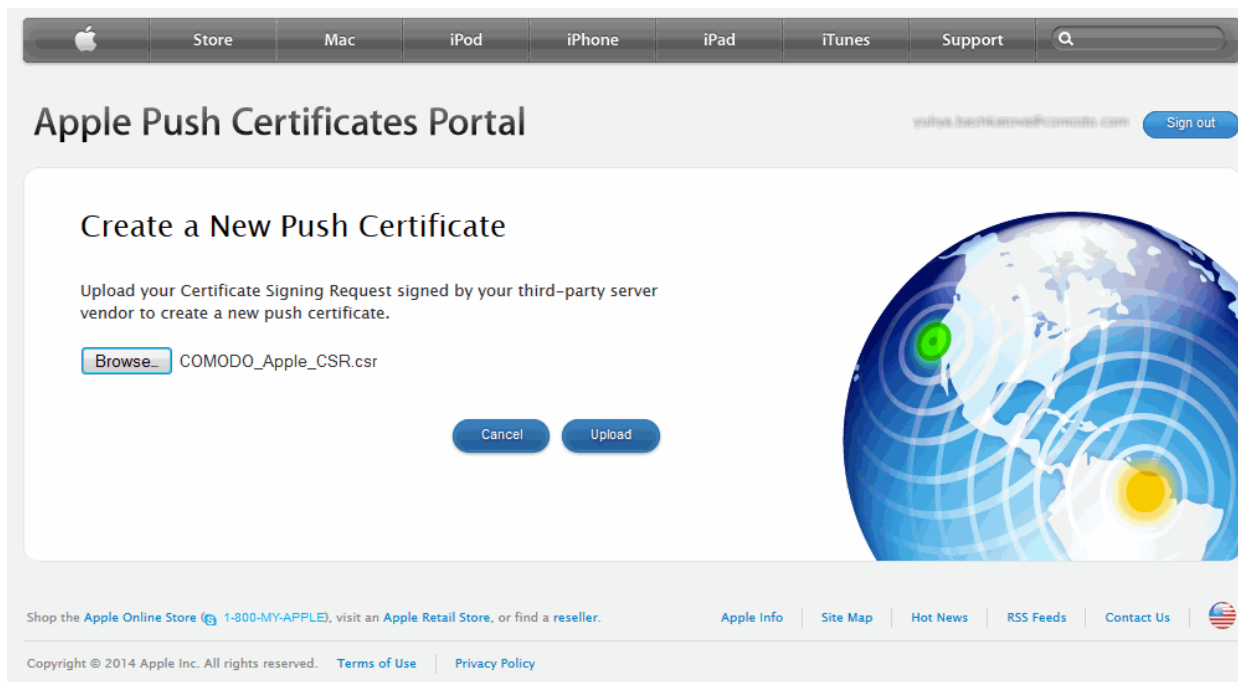
- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO\_Apple\_CSR.csr'. Please save this to your local drive.

## Step 2 –Obtain Your Certificate From Apple

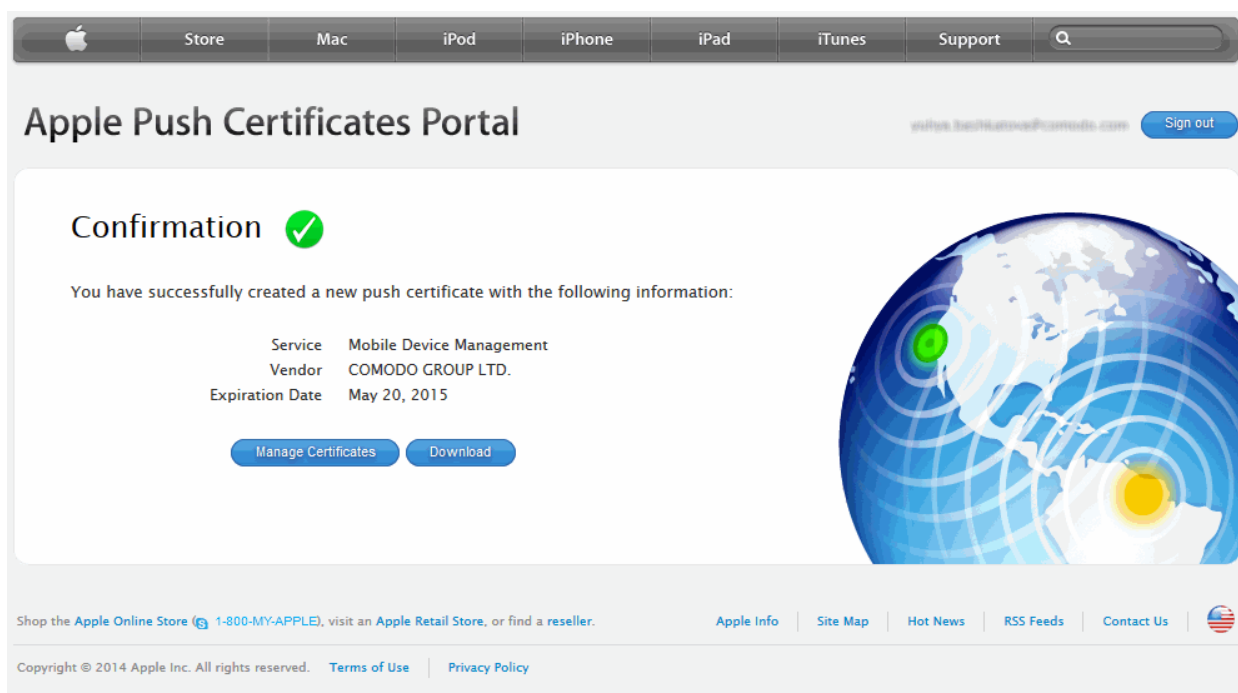
- Login to the 'Apple Push Certificates Portal' with your Apple ID at <https://identity.apple.com/pushcert/>. If you do not have an Apple account then please create one at <https://appleid.apple.com>.
- Once logged in, click 'Create a Certificate'. You will need to agree to Apple's EULA to proceed.



- On the next page, browse to the location where you stored 'COMODO\_Apple\_CSR.csr' and click 'Upload'.



- Apple servers will process your request and generate your push certificate. You can download your certificate at the confirmation screen:

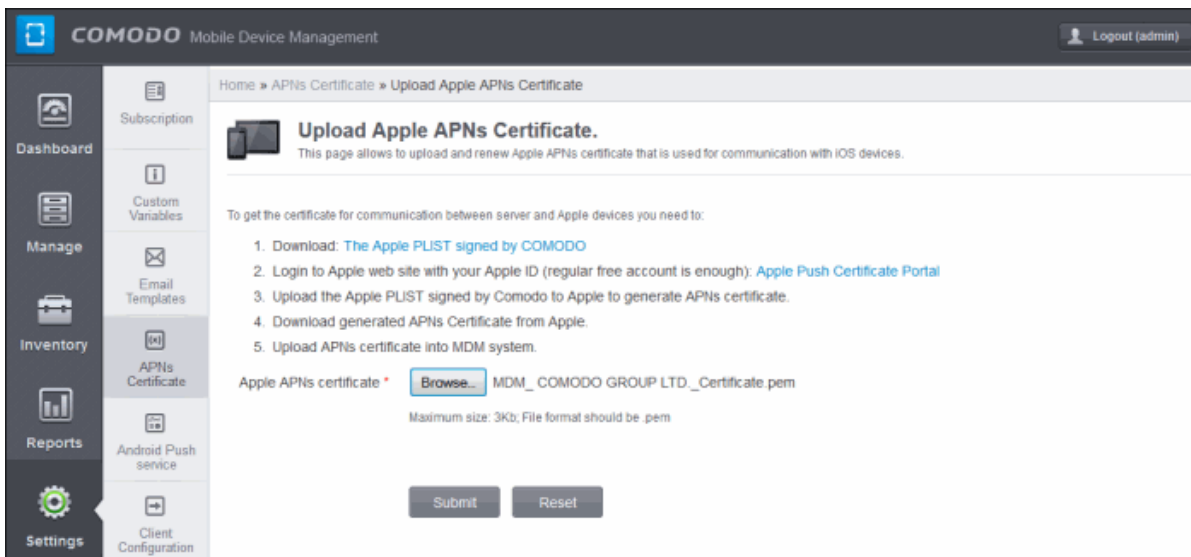


- Click the 'Download' button and save the certificate to a secure location. It will be a .pem file with a name similar to 'MDM\_COMODO GROUP LTD\_Certificate.pem'

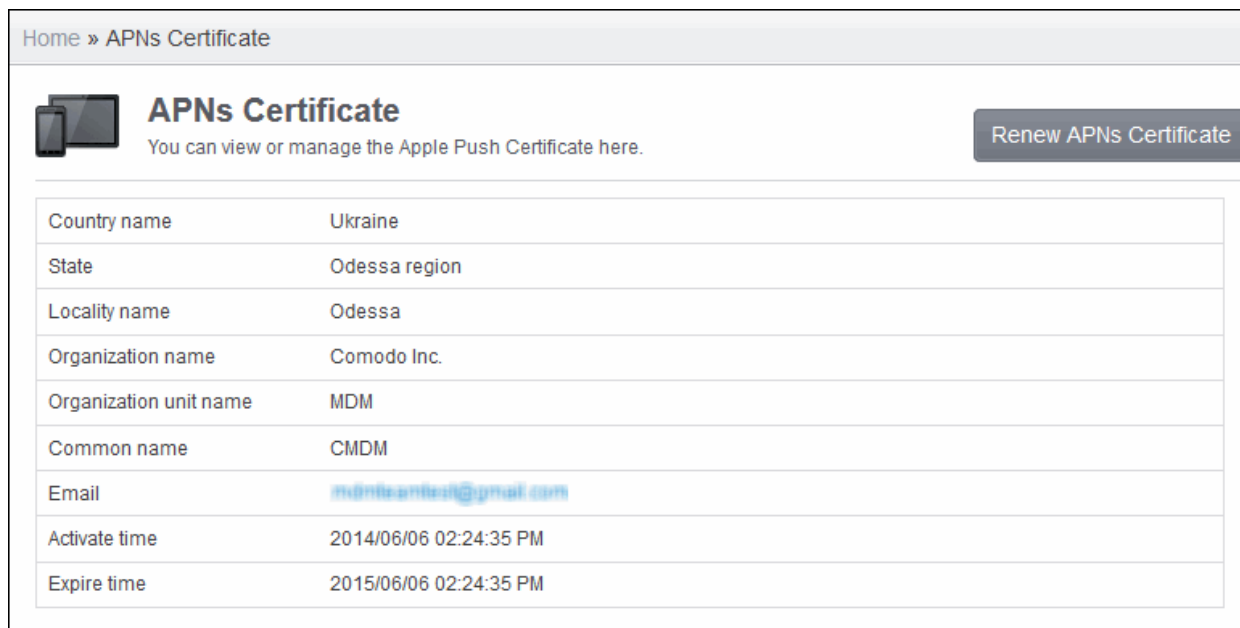
### Step 3– Upload your certificate to CMDM

- Next, return to the CMDM interface and open the APNs interface. Click the 'Browse' button to locate your certificate file then click 'Submit' to upload your certificate.





The APNs Certificate details interface will open:



CMDM will now be able to communicate with iOS devices.


The certificate is valid for 365 days. We advise you renew your certificate at least 1 week before expiry. If it is allowed to expire, you will need to re-enroll all your iOS devices to enable the server to communicate with them. To renew your APN Certificate, click the 'Renew APN Certificate' button.

## 7.4. Configuring Google Cloud Messaging (GCM) for Android

In order to communicate with enrolled Android devices, MDM server requires Google Cloud Messaging token to be installed in them. Comodo MDM ships with a default API token, which is used to communicate with enrolled Android devices. This default token is hardcoded and not visible in the interface. However, you can generate a unique Android GCM token that can be uploaded to MDM. To generate a GCM token, you must have created a Mobile Backend Project at <http://code.google.com/apis/console>.

## Start using the Google APIs console

to manage your API usage

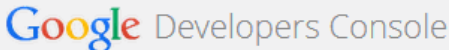



Creating an **APIs** project will let you:

- Use Google APIs **beyond anonymous limits**.
- **Monitor** API usage and **control** API access.
- **Share** API management with a team.

Create project...

- **Step 1** – Open Google API Console at <http://code.google.com/apis/console> and select Mobile Backend Project from the pull down menu at top left side. Click "CREATE PROJECT" button. Popup will appear where you need to fill project name and project id fields, check the check-boxes and click "Create" button.
- **Step 2** – After project is created project properties will be opened (if it is not - click on project name in the list).
- **Step 3** - Click "APIs & auth" and then select a sub menu "APIs".

< API Project

Overview

---

APIs & auth

APIs

Credentials

Consent screen

Push

---

Permissions

Settings


Support

---

Compute Engine

Cloud Storage

Cloud SQL

BigQuery 

Cloud Development

NAME	QUOTA	STATUS
Google Cloud Messaging for Android		<span style="background-color: green; color: white; padding: 2px 5px;">ON</span>
Ad Exchange Buyer API	1,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Ad Exchange Seller API	10,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Admin SDK	150,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
AdSense Host API	100,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
AdSense Management API	10,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Analytics API	50,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Audit API	10,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
BigQuery API	10,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Blogger API v3	10,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>
Books API	1,000 requests/day	<span style="background-color: #ccc; padding: 2px 5px;">OFF</span>

- **Step 4** – Find "Google Cloud Messaging for Android" in the list of available services and click the ON toggle.

Comodo Mobile Device Manager - Administrator Guide | © 2014 Comodo Security Solutions Inc. | All rights reserved

225



Google Cloud Messaging for Android

ON

[Quota](#) [Reports](#)

Google Cloud Messaging allows for push messaging to Android devices. [Learn more](#)

### Explore this API

Google Cloud Messaging for Android

- **Step 5** – Read and Accept the Terms of Services if you have not done so already.

Enable the Google Cloud Messaging for Android

I have read and agree to both [Google APIs Terms of Service](#) and [Google Cloud Messaging for Android Terms of Service](#).

[Accept](#) [Cancel](#)

- **Step 6** – Click "Credentials" under "APIs & auth" menu item.

**< API Project**

Overview

---

APIs & auth

APIs

**Credentials**

Consent screen

Push

**OAuth**

OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private.

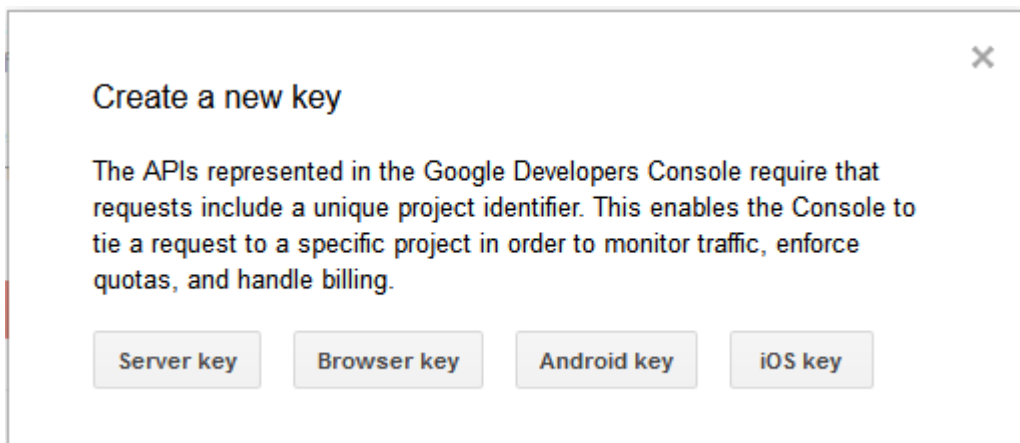
[Learn more](#)

[CREATE NEW CLIENT ID](#)

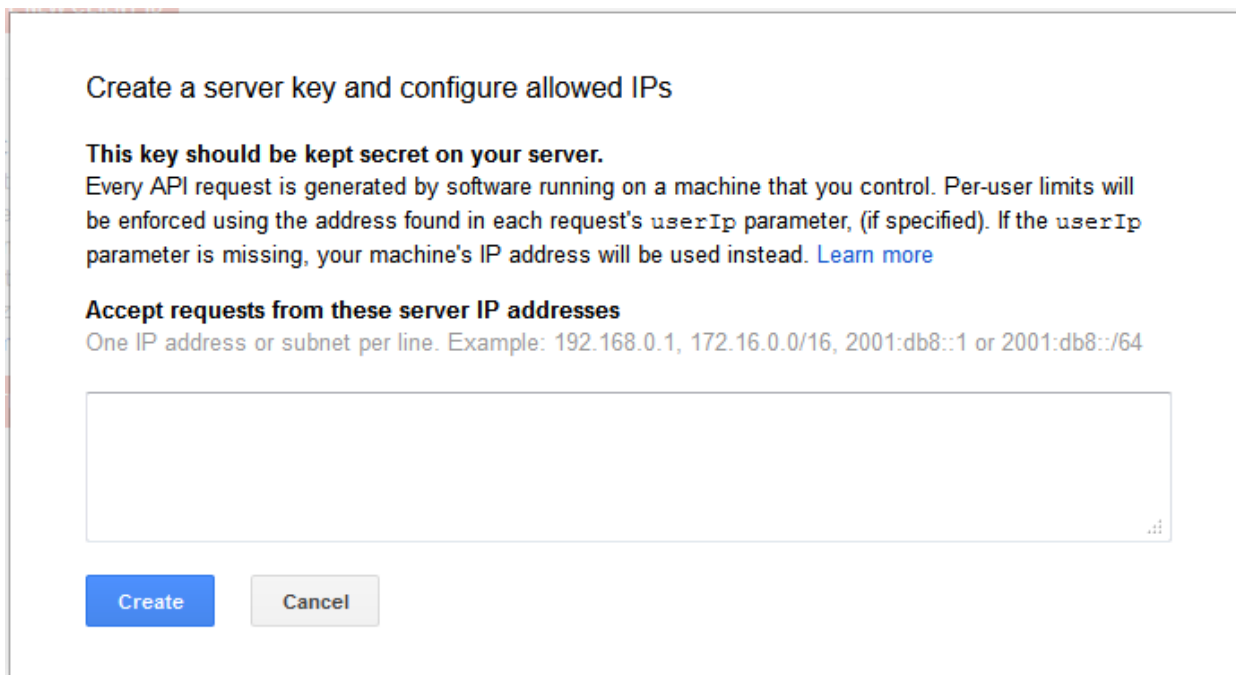
---

**Public API access**

- **Step 7** – Click "CREATE NEW KEY" button. In the appeared popup click "Server key" button. You don't need to supply any IP values in this form.



- **Step 8** – Click Create.



- **Step 9** - Copy the API key within the Key for server apps form.

### Key for server applications

API key	AIzaSyAL3bnP7TFRk118vv8p2R_DEF91g2B00FRk
IPs	Any IP allowed
Activation date	Apr 14, 2014 10:28 AM
Activated by	baahkatova7ul1ya@gmail.com (you)

- **Step 10** – Paste the API token to Android (GCM) Token field on MDM server portal.

Home » Add Google Cloud Messaging Token for Android.

### Add Google Cloud Messaging Token for Android.

Google Cloud Messaging (GCM for short) token enables MDM server to work with the Google Cloud Messaging Service that is required to communicate with Android devices.

**Android (GCM) Token \***

**Android (GCM) Project Number \***

Google Cloud Messaging for Android (GCM) is a service that allows you to send data from your server to your users' Android-powered device, and also to receive messages from devices on the same connection.

Before using GCM, you should navigate to [Google's API Console](#):

1. Click "CREATE PROJECT" button. Popup will appear where you need to fill project name and project id fields, check the check-boxes and click "Create" button
2. After project is created project properties will be opened (if it is not - click on project name in the list).
3. Click "APIs & auth" and then select a sub menu "APIs".
4. Find "Google Cloud Messaging for Android" in the list of available services and click the ON toggle.
5. Read and Accept the **Terms of Services** if you have not done so already.
6. Click "Credentials" under "APIs & auth" menu item.
7. Click "CREATE NEW KEY" button. In the appeared popup click "Server key" button. You don't need to supply any IP values in this form.
8. Click **Create**.
9. Copy the **API key** within the Key for server apps form.
10. Paste the **API token** to Android (GCM) Token field on MDM server portal.
11. Click "Overview" item in the top of left menu. Copy **Project number** in the top of page and paste to Android (GCM) Project number field on MDM server portal.

To get more information visit the following link: [https://developers.google.com/cloud/samples/mbs/android/enable\\_push](https://developers.google.com/cloud/samples/mbs/android/enable_push)

Until API key is synchronised with devices that are already enrolled Android Push Messages can arrive to devices with some delay.

- **Step 11** – Click "Overview" item in the top of left menu. Copy Project Number in the top of page and paste to Android (GCM) Project number field on MDM server portal. Click the 'Submit' button.

The settings is successfully updated dialog will be displayed.

## 7.5. Configuring the Android Agent

In order to retain the enrolled Android devices under the centralized management, it is imperative the agent in the device update CMDM server with all data The 'Client Configuration' interface allows the administrator to configure various settings that will be deployed onto the agent in the device.

### To open the 'Android Agent Settings' interface

- Click the 'Settings' tab from the left hand side and choose 'Client Configuration'.

**COMODO** Mobile Device Management

Home » Client Configuration

## Client Configuration

Client Configuration.

**Period for actual device information update \***

Hour(s)  
 Minute(s)

**Period for full device information update \***

Hour(s)  
 Minute(s)

**Period for antivirus database update \***

Hour(s)  
 Minute(s)

**Period for device events checking \***

Hour(s)  
 Minute(s)

**Period for checking profile restrictions on device to be active \***

Hour(s)  
 Minute(s)

**Siren Playing Duration \***

Minute(s)  
 Second(s)

**Password protection for uninstallation \***

**Distribute Certificates to Android?**

**Navigation Menu:**

- Dashboard
- Manage
  - Subscription
  - Custom Variables
  - Email Templates
- Inventory
  - APNs Certificate
- Reports
  - Android Push service
- Settings**
  - Client Configuration
  - Role Management
  - Active Directory
  - Anti-virus Settings
  - Pending Devices
  - Exchange Settings
  - Version

Client Configuration Settings	
Parameter	Description
Period for actual device information update	The update time interval for actual device information such as battery level, CPU usage, location of the device (GPS) and current WiFi SSID.
Period for full device information update	The update time interval for full device information such as memory status, name of the device, IMEI number, roaming state, MAC address of bluetooth and MAC address of WiFi.
Period for antivirus database update	The time intervals at which the antivirus database should be updated in the device.
Period for device events checking	The time interval at which the device should check MDM server for push notifications. Some of the push notifications from the MDM server may be missed. So the client will connect to the server for push notifications at time interval entered in this field.
Period for checking profile restrictions on device to be active	The time interval at which the client checks the device for profile restrictions. For example, if the use of camera is restricted,
Siren playing duration	Time duration the siren will play on devices when administrators activate the siren alarm.
Password protection for uninstallation	The password required for uninstalling the MDM app from the device.
Distribute Certificates to Android	If enabled, client certificates can be pushed to the devices via SCEP. The device user should allow the installation of the certificate on the device.

- Enter the parameters in the fields and click the 'Save' button.

The settings will be saved and the success message will be displayed.

The settings is successfully updated.

- Click the 'Inform devices now' button for the settings to take effect immediately on the Android client in the enrolled devices.

## 7.6. Configuring the Role-Based Access Control for Users

Users that are added to Comodo Mobile Device Manager (CMDM) have administrative privileges and access to different areas of the interface, depending on the role assigned to them. The Role Management interface renders switchable Roles/Users interfaces, that allow the administrator to manage the roles and manage the roles assigned to users.

To open the 'Roles/Users' interface, click the 'Settings' tab from the left hand side and choose 'Role Management'.

Home » Roles

## Roles / Users

Create new Role

Name	Description	Members	[set as default]	
role2	role2	Members	[set as default]	🔍
Administrators	Administrators of the system	Members	[set as default]	🔍
Field Sales Representative	Employees with limited privileges	Members	[set as default]	🔍

Results per page: 20

## Roles

The Roles interface allows the administrator to create various roles including administrative roles with different access permissions and privilege levels as required, for various departments in an organization and user roles with limited privilege levels. The roles created through this interface will be available for selection while adding a new user, enabling assigning the appropriate role to the new user. The administrator can add more roles or remove assigned roles to a user at a later time.

One of the roles created through this interface can be set as a default role. When a new user is added, the default role will be assigned to him/her, if no role is not selected by the administrator. The user can be assigned with a different role, at a later time, as required.

To switch to Roles interface, click on the 'Roles' tab.


Home » Roles

## Roles / Users

Create new Role

Name	Description	Members	[set as default]	
role2	role2	Members	[set as default]	🔍
Administrators	Administrators of the system	Members	[set as default]	🔍
Field Sales Representative	Employees with limited privileges	Members	[set as default]	🔍

Results per page: 20

Roles - Column Descriptions		
Column Heading		Description
Name		The name of the role.
Description		The short description of the role.
Controls Buttons	Members	Enables the administrator to view the members assigned to the role. Refer to the section <b>'Managing Permissions and Assigned Users of a Role' &gt; 'Viewing the users assigned with the role'</b> for more details.
	[Set as Default]	Enables the administrator to set the role as default role. The role set as default, is indicated as '[Default]' in this column.
		Enables the administrator to view the permissions assigned to the role, edit the role, manage the permissions, manage the users belonging to the role and delete the role. Refer to the section <b>'Managing Permissions and Assigned Users of a Role'</b> for more details.

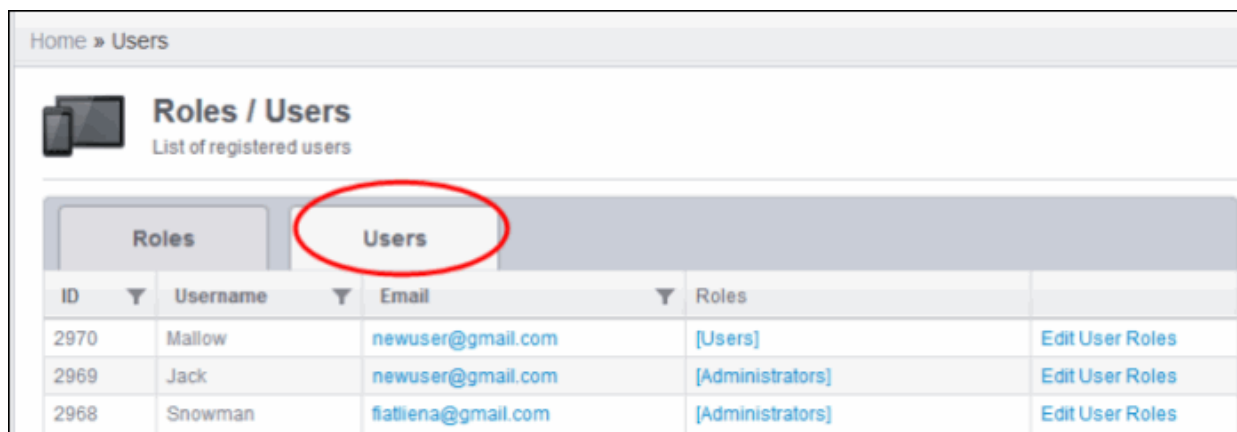
From the Roles interface, the administrator can:

- **Create a new role**
- **Manage a Role**
  - Edit a role name and description of a role
  - Manage the permissions assigned to a role
  - Manage the users assigned with a role
- **Remove a Role**

## Users

The Users interface allows the administrator to view the list of users added to CMDM and the roles assigned to them. The administrator can also add or remove the roles assigned to each user from this interface.

To switch to Roles interface, click on the 'Users' tab.



Users - Column Descriptions	
Column Heading	Description
ID	The Identity Number assigned to the user.
Username	The Login username of the user.
Email	The registered email address of the user.



Roles	The roles assigned to the user. Clicking on a role opens the management pane of the role. Refer to the section ' <b>Managing Permissions and Assigned Users of a Role</b> ' for more details.	
Controls Buttons	Edit User Roles	Enables the administrator to add or remove roles assigned to a user. Refer to the section ' <b>Managing Roles assigned to a User</b> ' for more details.

The Users interface allows the administrator to:

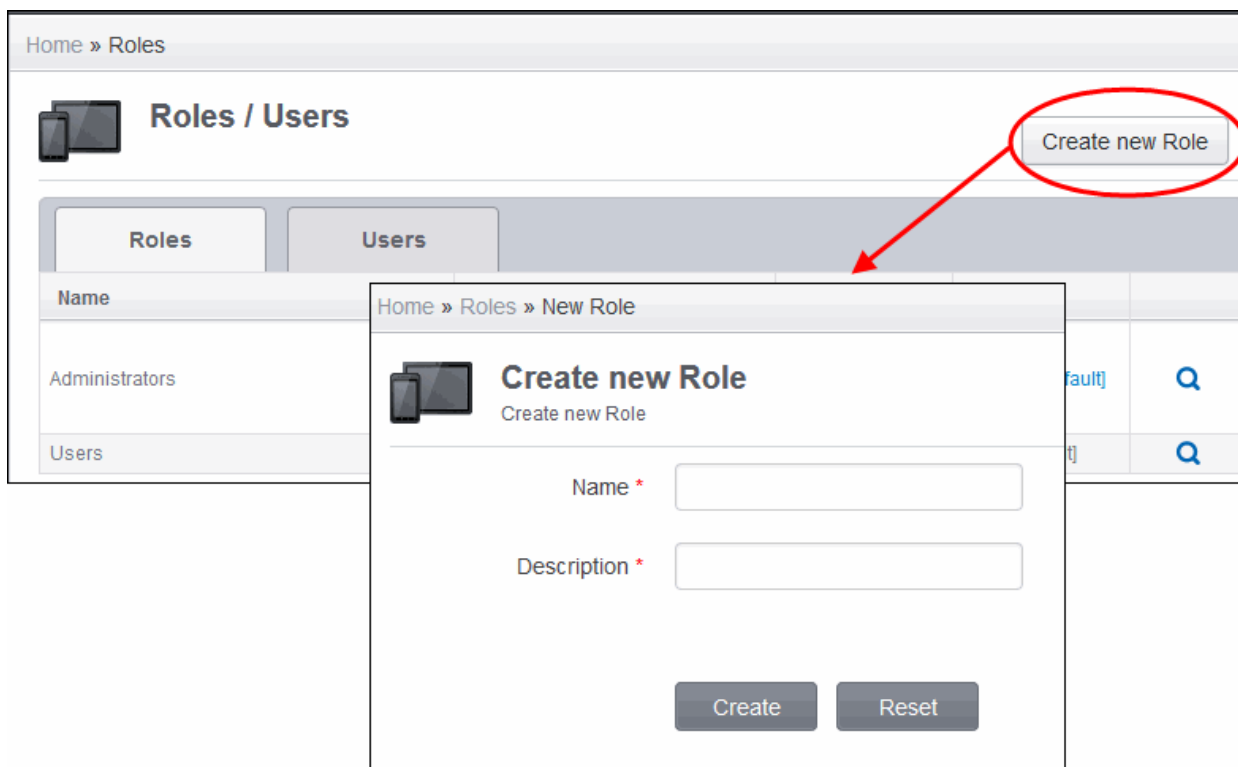
- **Add or Remove roles to a user**

## 7.6.1. Creating a New Role

The administrator can create several roles with different permissions and privilege levels for administrators and users belonging to different departments of an organization.

### To create a new role

- Click the 'Settings' tab from the left hand side and choose 'Role Management'.
- Click the 'Roles' tab.
- Click the 'Create new Role' button at the top right of the interface.



The Create new Role wizard will start.

- Enter an appropriate name for the role to be created in the 'Name' text box.
- Enter a short description for the role in the 'Description' text box.
- Click 'Create'.

The new role will be created and the 'Edit Role Permissions' interface will open.

- Select the permissions to be assigned for the new role.

Home » Roles » Sales Department » Edit » Permissions

## Sales Department: Edit Role Permissions

Permissions for employees

Edit Name/Description

View Role

---

**Add or remove permissions from a role**

<input type="checkbox"/>	Permission	Description
<input type="checkbox"/>	audit.compliance	Access to compliance page
<input type="checkbox"/>	audit.push	Access to push statistic page
<input type="checkbox"/>	audit.threats	Access to threats report page
<input type="checkbox"/>	audit.user-activity&devices	Access to user activity and devices report page. Child permission is: "inventory.devices".
<input type="checkbox"/>	dashboard	Access to dashboard part of the system
<input type="checkbox"/>	inventory.access-ms-exchange	MS Exchange access management. Child permission is: "inventory.devices.manage", "inventory.users.manage".
<input type="checkbox"/>	inventory.antivirus	Access right to antivirus (full control). Child permissions are: "inventory.devices" and "audit.threats".
<input type="checkbox"/>	inventory.devices	Access to devices part (read only)
<input type="checkbox"/>	inventory.devices.actions	Actions with devices. Child permission is: "inventory.devices".
<input type="checkbox"/>	inventory.devices.applications	Access to application on devices part (read only). Child permission is: "inventory.devices".
<input type="checkbox"/>	inventory.devices.applications.manage	Access to application on devices part (full control). Child permissions are: "inventory.devices" and "inventory.devices.applications".
<input type="checkbox"/>	inventory.devices.enroll	Grant enroll permission. Child permission is: "inventory.users".
<input type="checkbox"/>	inventory.devices.manage	Manage devices (full control). Child permission is: "inventory.devices".
<input type="checkbox"/>	inventory.users	Access to users part (read only)
<input type="checkbox"/>	inventory.users.manage	Manage users (full control). Child permission is: "inventory.users".
<input type="checkbox"/>	manage.applications-repository	Manage application repository
<input type="checkbox"/>	manage.profiles	Manage Profiles (read only)
<input type="checkbox"/>	manage.profiles.association	Association profiles with devices. Child permissions are: "manage.profile", "inventory.devices.manage" and "inventory.users".
<input type="checkbox"/>	manage.profiles.manage	Manage Profiles (full control). Child permissions are: "manage.profiles" and "inventory.devices".
<input type="checkbox"/>	settings.active-directory	Manage LDAP account. Child permission is: "settings.rbac".
<input type="checkbox"/>	settings.android-push-service	Manage Google API token.
<input type="checkbox"/>	settings.antivirus	Manage antivirus settings
<input type="checkbox"/>	settings.apns-certificate	Manage Apple Push Notification service certificate.
<input type="checkbox"/>	settings.client-configuration-android	Manage android settings
<input type="checkbox"/>	settings.eas-token	Manage EAS token.
<input type="checkbox"/>	settings.email-templates	Manage email templates.
<input type="checkbox"/>	settings.rbac	Access to RBAC (read only). Child permission is: "inventory.users".
<input type="checkbox"/>	settings.rbac.manage	Access to RBAC (full control). Child permission is: "settings.rbac".
<input type="checkbox"/>	settings.subscription	Access to Subscription section.

Total 29 results.

Save

- If you want to edit the role name or description, click 'Edit Name / Description' from the top left and make your

changes.


- Click 'Save' for your changes to take effect.

The new role will be created and will be available for assigning to a new or existing user.


## 7.6.2. Managing Permissions and Assigned Users of a Role

The administrator can view and modify any role created in the CMDM at any time from the Roles interface.

### To view and manage a role

- Click the 'Settings' tab from the left hand side and choose 'Role Management'.
- Click the 'Roles' tab.
- Click the magnifier icon  in the row of the role to view the details of a role.

Home » Roles » Sales Manager



### Sales Manager: Details

Admin for devices in Sales Dept

Action ▾

Delete

Name	Sales Manager	
Description	Admin for devices in Sales Dept	
Default	No	
Role Permissions		
	audit.compliance	Access to compliance page
	audit.user-activity&devices	Access to user activity and devices report page. Child permission is: "inventory.devices".
	dashboard	Access to dashboard part of the system
	inventory.antivirus	Access right to antivirus (full control). Child permissions are: "inventory.devices" and "audit.threats".
	inventory.devices	Access to devices part (read only)
	inventory.devices.actions	Actions with devices. Child permission is: "inventory.devices".
	inventory.devices.applications.manage	Access to application on devices part (full control). Child permissions are: "inventory.devices" and "inventory.devices.applications".
	inventory.devices.enroll	Grant enroll permission. Child permission is: "inventory.users".
	inventory.devices.manage	Manage devices (full control). Child permission is: "inventory.devices".
	inventory.users	Access to users part (read only)
	inventory.users.manage	Manage users (full control). Child permission is: "inventory.users".
	audit.threats	Access to threats report page
	inventory.devices.applications	Access to application on devices part (read only). Child permission is: "inventory.devices".

The View Role interface allows the administrator to:

- **Edit the name and description of the role**
- **Manage the permissions assigned to the role**
- **View the users assigned with the role**
- **Assign the role to selected users**
- **Remove a role from selected users**

## To edit a role name and description of the role

- Click 'Action' from the top right and choose 'Edit'. The Edit Role interface will open.

The image shows two screenshots of the Comodo Mobile Device Manager interface. The top screenshot is the 'Sales Manager: Details' page, which includes a breadcrumb trail 'Home » Roles » Sales Manager', a title 'Sales Manager: Details' with the subtitle 'Admin for devices in Sales Dept', and an 'Action' dropdown menu. The dropdown menu is open, showing options: 'Edit', 'Role Permissions', 'Members', 'Assign members', and 'Revoke members'. The 'Edit' option is highlighted in blue. Below this is a table with columns for 'Name', 'Description', 'Default', and 'Role Permissions'. The 'Role Permissions' section lists 'audit.compliance', 'audit.user-activity&devices', and 'dashboard' with their respective descriptions. The bottom screenshot is the 'Edit: Sales Manager' page, with a breadcrumb trail 'Home » Roles » Sales Manager » Edit'. It features a title 'Edit: Sales Manager' and subtitle 'Admin for devices in Sales Dept'. There are two buttons: 'Edit Permissions' and 'View Role'. Below these are two text input fields: 'Name \*' containing 'Sales Manager' and 'Description \*' containing 'Admin for devices in Sales Dept'. A note states 'Fields with \* are required.' At the bottom are 'Save' and 'Cancel' buttons.

- To change the name of the role, enter the new name in the name text box
- To change the description of the role, enter the new role in the Description text box.
- If you want to change the permissions assigned to the role, click 'Edit Permissions' from the top right. The Manage Role interface will open. Refer to the section '**To manage the permissions assigned to a role**' below for more details.
- Click 'Save' for your changes to take effect.

## To manage the permissions assigned to the role

- Click 'Action' from the top right and choose 'Role Permissions'. The 'Edit Role Permissions' interface will open.

Home » Roles » Sales Manager

## Sales Manager: Details

Admin for devices in Sales Dept

Action 
Delete

Name	Sales Manager	
Description	Admin for devices in Sales Dept	
Default	No	
Role Permissions	audit.compliance	Access to compliance page
	audit.user-activity&devices	Access to user activity and devices report page. Child permission is: "inventory devices".
	dashboard	Access to dashboard part of the system

## Sales Manager: Edit Role Permissions

Admin for devices in Sales Dept

Edit Name/Description
View Role

**Add or remove permissions from a role**

<input type="checkbox"/>	Permission	Description
<input checked="" type="checkbox"/>	audit.compliance	Access to compliance page
<input checked="" type="checkbox"/>	audit.threats	Access to threats report page
<input checked="" type="checkbox"/>	audit.user-activity&devices	Access to user activity and devices report page. Child permission is: "inventory devices".

- Select the new permissions to be assigned to the role.
- Deselect the permissions to be removed from the role.
- Click 'Save' for your changes to take effect.

**To view the list of users assigned with the role**

- Click 'Action' from the top right and choose 'Members'. The 'Members' interface will open.

Home » Roles » Sales Manager

## Sales Manager: Details

Admin for devices in Sales Dept

Action ▼ Delete

Name	Sales Manager		
Description	Admin for devices in Sales Dept		
Default	No		
Role Permissions	audit.compliance	Access to com	
	audit.user-activity&devices	Access to user permission is:	ge. Child
	dashboard	Access to dashboard part of the system	

Edit

Role Permissions

Members

Assign members

Revoke members

Home » Roles » Sales Manager » Members

## Members: Sales Manager

List of users with this role View Role

ID	Username	Email	
2969	Jack	newuser@gmail.com	<a href="#">Edit User Roles</a>
2968	Snowman	fiatliena@gmail.com	<a href="#">Edit User Roles</a>

Results per page: 20 Displaying 1-2 of 2 results.

- To add or remove roles assigned to a user, click the 'Edit User Roles' link in the row of the user. Refer to the section **Managing Roles assigned to a User** for more details.

### To assign the role to selected users

- Click 'Action' from the top right and choose 'Assign members'. The 'Assign Role to Users' interface will open.

Home » Roles » Sales Manager

## Sales Manager: Details

Admin for devices in Sales Dept

Action ▼ Delete

Name	Sales Manager		
Description	Admin for devices in Sales Dept		
Default	No		
Role Permissions	audit.compliance	Access to com	
	audit.user-activity&devices	Access to user permission is:	ge. Child
	dashboard	Access to dashboard part of the system	

Edit

Role Permissions

Members

Assign members

Revoke members

Home » Roles » Sales Manager » Assign members

## Assign 'Sales Manager' Role to Users

Users on this page are not currently members of this role

<input type="checkbox"/>	ID	Username	Email	Roles	
<input checked="" type="checkbox"/>	2970	Mallow	newuser@gmail.com	[Users]	<a href="#">Edit User Roles</a>
<input type="checkbox"/>	2958	User2014721215320	test.selenium.mdm@gmail.com	[Selenium_testing2014313-16-12-58]	<a href="#">Edit User Roles</a>
<input type="checkbox"/>	2954	User2014721214612	test.selenium.mdm@gmail.com	[Selenium_testing2014313-16-12-58]	<a href="#">Edit User Roles</a>

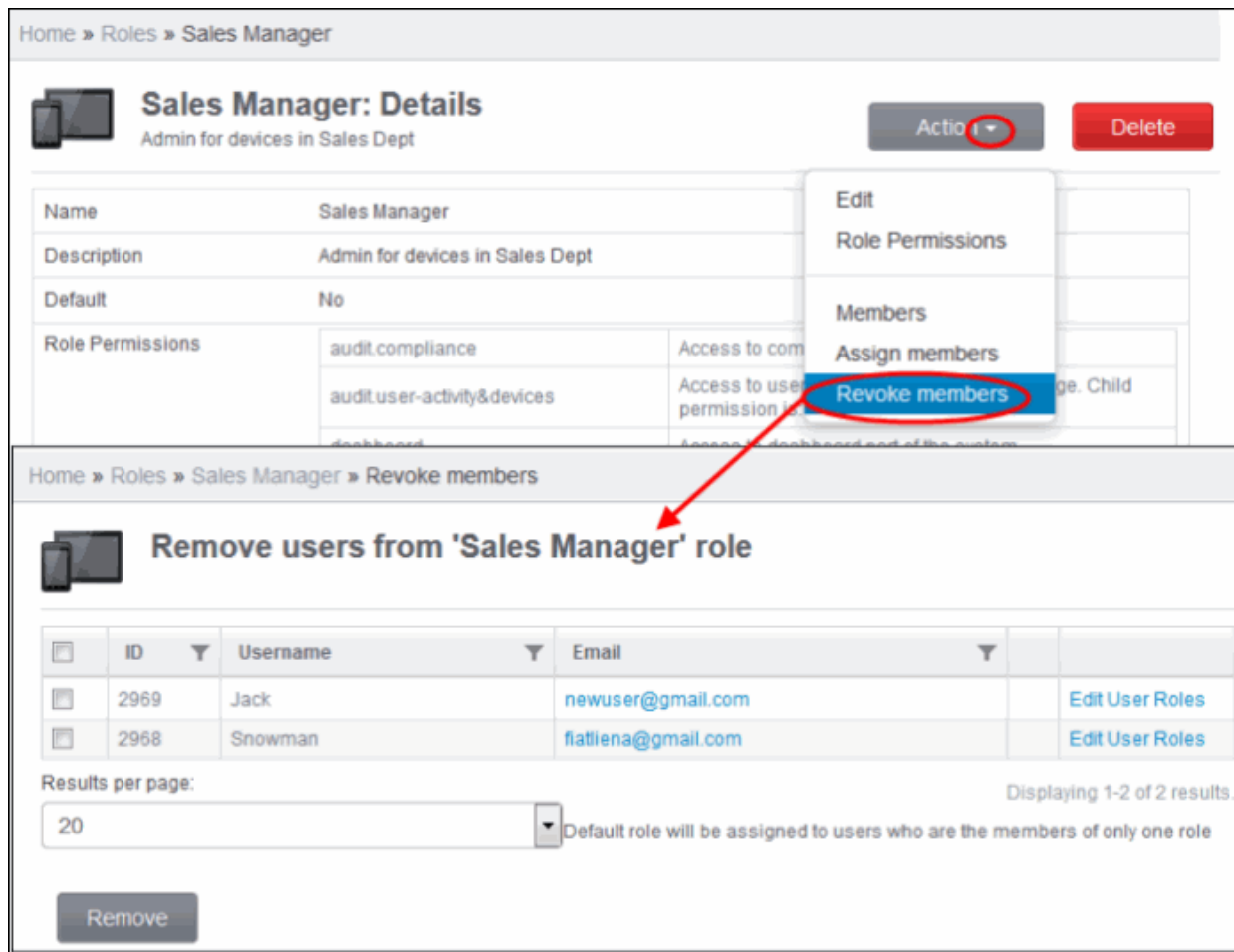
The interface will display all the users enrolled to CMDM, but not assigned with the selected role.

- Select the users to whom the role needs to be assigned.
- Click 'Assign'. The role will be assigned to the selected users.

**Tip:** The administrator can click the 'Roles management' link in the row of a user to add or remove roles assigned to a user. Refer to the section **Managing Roles assigned to a User** for more details.

### To remove the role from selected users

- Click 'Action' from the top right and choose 'Revoke members'. The 'Remove user role' interface will open.



The interface will display a list of all the users assigned with the selected role.

- Select the users to whom the role needs to be removed.
- Click 'Remove'. The role will be removed from the selected users.


**Tip:** The administrator can click the 'Edit User Role' link in the row of a user to add or remove roles assigned to a user. Refer to the section **Managing Roles assigned to a User** for more details.

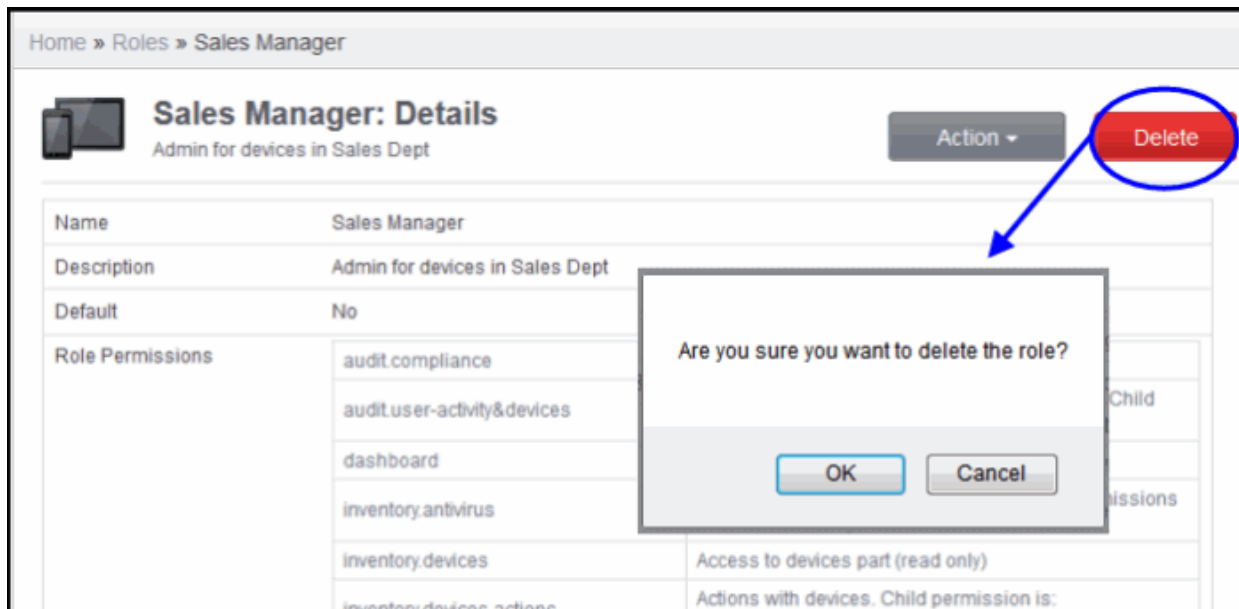
## 7.6.3. Removing a Role

If required, the administrator can remove roles that are no longer deemed necessary. Once a role is removed, it will be stripped from the privileges of the users to whom it was assigned. Administrators should confirm they wish to remove a role entirely rather than remove a role from specific users.



## To remove a role

- Click the 'Settings' tab from the left hand side and choose 'Role Management'.
- Click the 'Roles' tab.
- Click the magnifier icon  in the row of the role to view the details of a role.



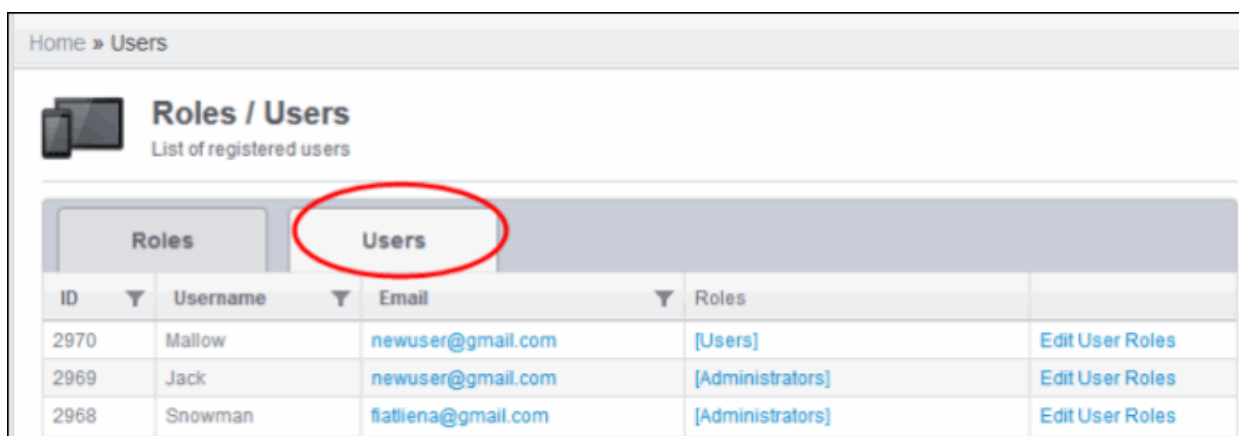
- Click the 'Delete' button at the top right. A confirmation dialog will appear.
- Click OK to remove the role.

## 7.6.4. Managing Roles assigned to a User

The 'Users' interface allows the administrator to add new roles and to remove roles assigned to a user.

To open the Users interface

- Click the 'Settings' tab from the left hand side and choose 'Role Management'.
- Click the 'Users' tab.



## To manage roles assigned to a user

- Click the 'Edit User Roles' link in the row of the selected user. The 'Edit Roles' interface will open.

Home » Users » Bob

**Edit Roles: Bob**  
Assign roles to the selected user

<input type="checkbox"/>	name
<input checked="" type="checkbox"/>	Administrators
<input type="checkbox"/>	Users
<input type="checkbox"/>	Field Sales Representative
<input type="checkbox"/>	Demo
<input type="checkbox"/>	Store Assistant

Displaying 1-5 of 5 results.

Save

The roles assigned to the user will be listed.

- To add a new role to the user, select the role from the list.
- To remove a role for the user, deselect the checkbox beside the role.
- Click 'Save' for your changes to take effect.

## 7.7. Importing User Groups from LDAP

In addition to adding user groups manually, CMDM enables the administrators to import user groups from the Active Directory (AD) server of the domain. You can configure CMDM to access your AD server through Lightweight Directory Access Protocol (LDAP) to import the user groups.

To open the 'Active Directory' interface, click the 'Settings' tab from the left hand side and choose 'Active Directory' and select the 'Enable LDAP' checkbox.

The screenshot displays the Comodo Mobile Device Manager web interface. The top navigation bar includes the Comodo logo and the text "COMODO Mobile Device Management". A breadcrumb trail shows "Home » Active Directory settings". The left sidebar contains a vertical menu with icons and labels for "Dashboard", "Manage", "Inventory", "Reports", and "Settings". The "Settings" menu item is highlighted. The main content area is titled "Active Directory settings" and features a "Save and next" button. The settings include:

- Subscription**
- Custom Variables**
- Email Templates**
- APNs Certificate**
- Android Push service**
- Client Configuration**

The "Active Directory settings" section includes:

- Active Directory settings**
- Enable LDAP \***
- LDAP server host \*** (text input field)
- LDAP account rdn \*** (text input field)
- LDAP account password \*** (text input field)

A "Save and next" button is located at the bottom of the settings section.

- **LDAP Server** – Enter the IP of LDAP server.
- **LDAP Account RDN** – Enter the relative distinguished name (RDN) of the LDAP account separated by commas. For example, CN=Smith,CN=Users,DC=example,DC=com
- **LDAP Account Password** – Enter the password for the LDAP account.

Home » Active Directory settings



## Active Directory settings

Active Directory settings

Enable LDAP \*

LDAP server \*

11.111.111.11

LDAP account rdn \*

CN=James,CN=Users,DC=example,DC=com

LDAP account password \*

••••••

Save and next

- Click the 'Save and next' button.

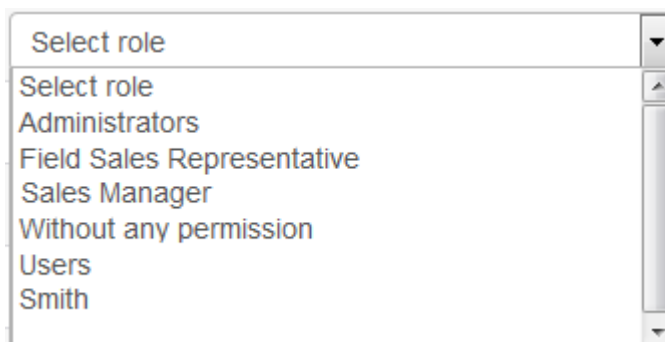
The groups in AD will be displayed.

Name	
Enterprise Read-only Domain Controllers	Select role ▼
vadym_test_group	Select role ▼
KirillGroup	Administrators ▼
WinRMRemoteWMIUsers__	Select role ▼
DnsUpdateProxy	Select role ▼
DnsAdmins	Select role ▼
Denied RODC Password Replication Group	Select role ▼
Allowed RODC Password Replication Group	Select role ▼
RAS and IAS Servers	Select role ▼
Read-only Domain Controllers	Select role ▼
Group Policy Creator Owners	Select role ▼
Enterprise Admins	Select role ▼
Schema Admins	Select role ▼
Cert Publishers	Select role ▼
Domain Controllers	Select role ▼
Domain Computers	Select role ▼
Domain Guests	Select role ▼
Domain Users	Select role ▼
Domain Admins	Select role ▼

Back

Save and next

- If required, select the roles that you want to assign the users in a group from the 'Select role' drop-down beside a group.



If no role is selected for the users at this stage, the users in the group will be assigned default roles that can see only server version section.

- Click 'Save and next'.

Home » Active Directory settings

## Active Directory settings

---

Active Directory settings

**Add users but don't add their devices automatically \***

Back
Save and send

- **Add users but don't add their devices automatically** – If selected, users in the groups will not be able to enroll their devices. To do so, the users will have to first login into the application using their LDAP credentials (this will add them to MDM) and administrators will have to send enrollment email for the users from User's page. On successful enrollment, the users will be available in the respective group imported from LDAP.

If the 'Add users but don't add their devices automatically' checkbox is deselected, administrators can select the number of devices that users can enroll and choose not to send any enrollment mails, send enrollment mails to all or enter users' email addresses / alias email addresses, each address separated by a comma. However, the users will not be added into their respective group unless they authenticate themselves with their LDAP credentials in the page after clicking the second link in the enrollment mail.

Home » Active Directory settings

## Active Directory settings

---

Active Directory settings

**Add users but don't add their devices automatically \***

---

**Count auto enroll devices**

5

Do not send any enrollment mail

Send enrollment mails to everyone

Mail addresses that receive notification for device enrollment, comma-separated

ser1example.com, user2@gmail.com

Back
Save and send

- Click the 'Save and send' button.

The 'Changes saved' info will be displayed and mails sent to users automatically as per the selection.



The user groups will be imported into MDM and can be viewed by clicking Inventory > User groups. The users will be added into their respective group only after they authenticate themselves with their LDAP credentials in the page after clicking the second link in the enrollment mail.

Home » Group users

### Group users list

	ID	Group name	Creator user	Time creation	Last modified user
<input type="checkbox"/>	3	Smith	asli	2014/06/25 02:12:10 AM	✘

Results per page:  Displaying 1-4 of 4 results.

Manage Profiles
Create user group

Refer to the section '[Managing User Groups](#)' for more details on User Groups.

Refer to the section '[Managing Users](#)' for more details on Users.

## 7.8. Antivirus Settings

The CMDM Agent installed on Android smart phones and tablets provide 'Always on' antivirus protection by performing real-time/on-access scanning every time a file is copied or downloaded to the device or an app is installed on the device. The administrator can also launch On-Demand scans from the CMDM administrative console on selected devices.

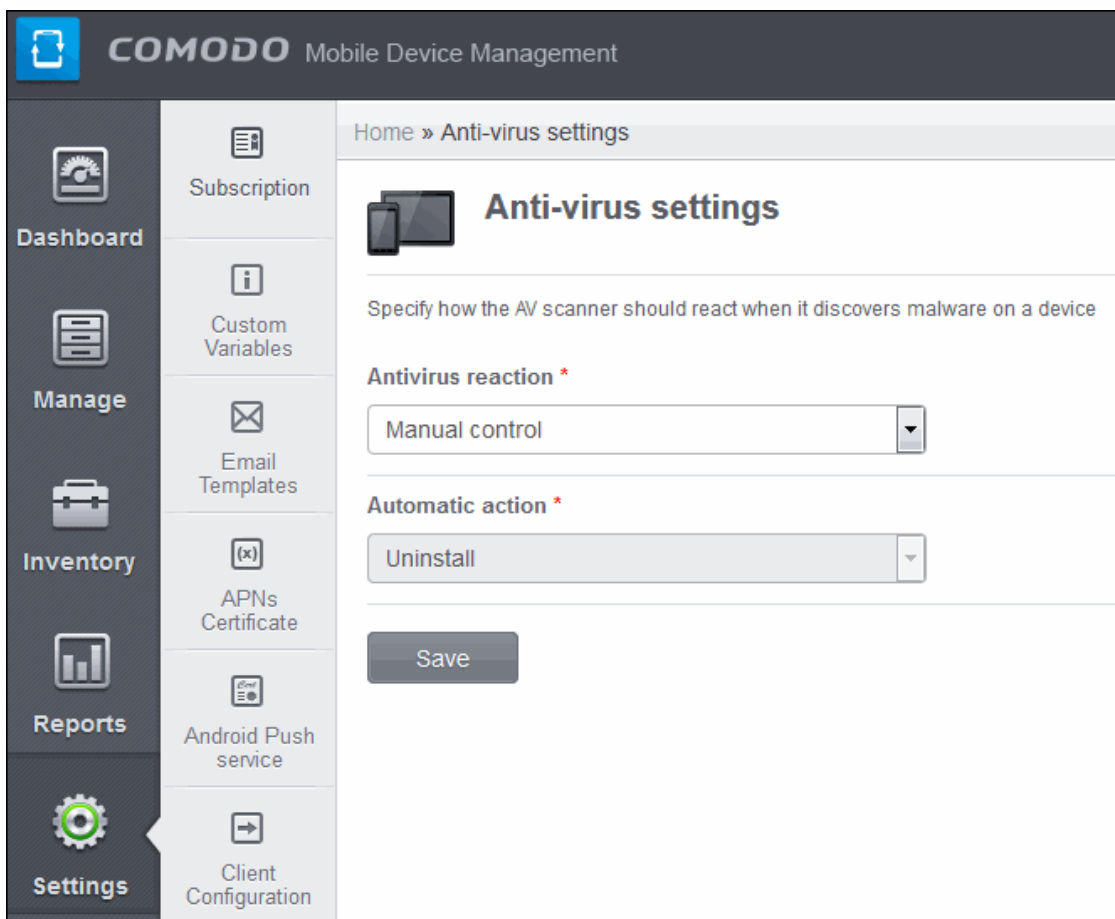
The administrator can configure whether the malware, virus and other threats identified by the on-access or on-demand scans are to be automatically removed or to be manually cleaned.

- If automatic control is chosen, the CMDM agent can automatically uninstall the app containing the virus or ignore as set from the console.
- If manual control is chosen, the status of the device will be indicated as 'Infected' at the console, on identifying a virus and a notification will be displayed on the device. The user can respond to the notification to manually remove the virus. Refer to the section [Running On-demand Antivirus Scans on Enrolled Devices](#) for more details.

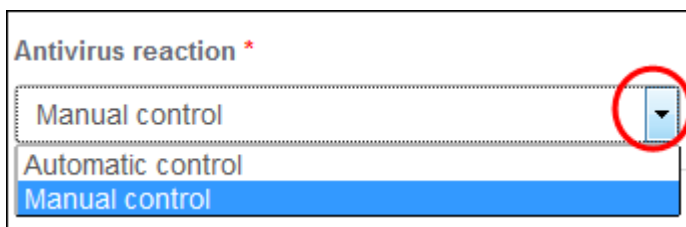
The Antivirus settings interface allows the administrator to configure how the agent should behave if a malware, virus or other threat is identified at the end of an on-access or on-demand scan.

To open the 'Antivirus settings' interface, click the 'Settings' tab from the left hand side and choose 'Antivirus Settings'.



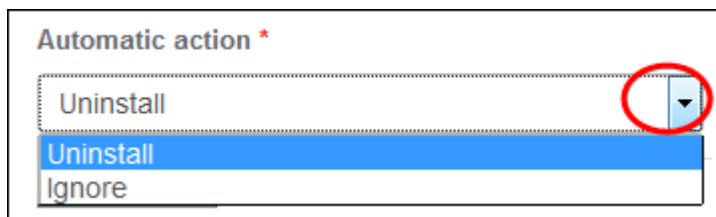


- **Antivirus Reaction** - The administrator can choose whether the identified virus needs to be acted upon automatically or manually from the 'Antivirus Reaction' drop-down.



If Manual Control is chosen, then the administrators have the option to take appropriate action on threats detected in the AV Scan interface. Refer to the section **Managing Antivirus and Running Scans on Enrolled Devices** for more details.

- **Automatic Action** - If 'Automatic control' is chosen from the 'Antivirus Reaction' drop-down, the administrator can select whether the identified virus is to be ignored, uninstalled or moved to quarantine.



- Click 'Save' for your settings to take effect.

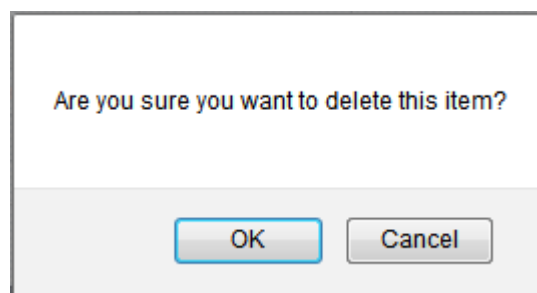
## 7.9. Viewing and Managing Removed Devices

When a device is removed from the 'Devices inventory' screen, CMDM sends a command to the device and gets a confirmation from it. If the user has already uninstalled the app on the device then there will be no confirmation from the device for the command. The devices that do not respond to removal command from CMDM will be listed in the Devices Pending Removal screen. The devices in the Devices Pending Removal list cannot be enrolled again unless they are removed from the list.

To open the removal confirmation list, click the 'Settings' tab from the left hand side and choose 'Removal Confirmation'. The Devices interface with a list of devices removed from CMDM but with no response from them will be displayed.

- To confirm the removal of a device, click the 'Delete' icon **X** in the row of the device.

A confirmation dialog will appear.



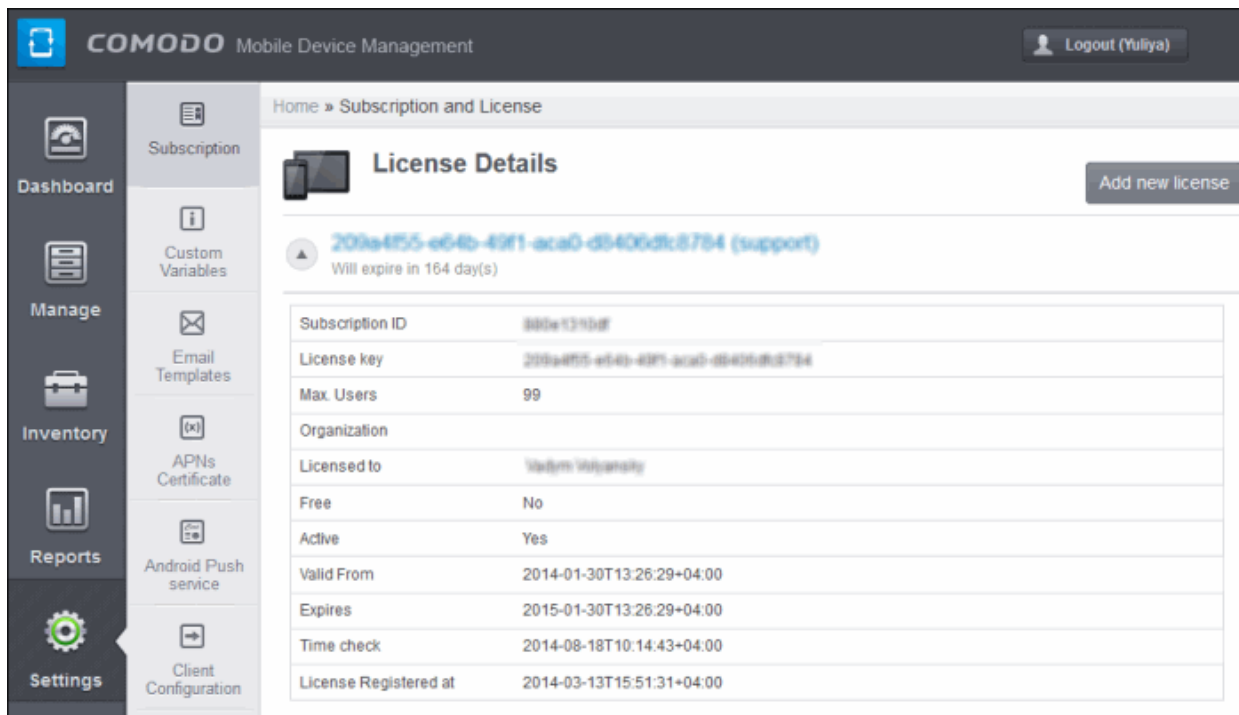
- Click 'OK' to remove the device.

Now these devices can be enrolled again in CMDM if required.

## 7.10. Viewing and Managing Licenses

The 'Subscription and License' panel displays the details on the licenses purchased, their type and validity status, number of users allowed, number of devices that can be enrolled and so on. The 'License Information' screen also allows the administrator to add new licenses purchased for adding more number of devices and users in their account.

To open the 'Subscription and License' panel, click the 'Settings' tab from the left hand side and choose 'Subscription'.



## 7.10.1. Upgrading or Adding the License

Administrators can add more users to their account by upgrading their license in the Comodo account management portal.

### To upgrade a license

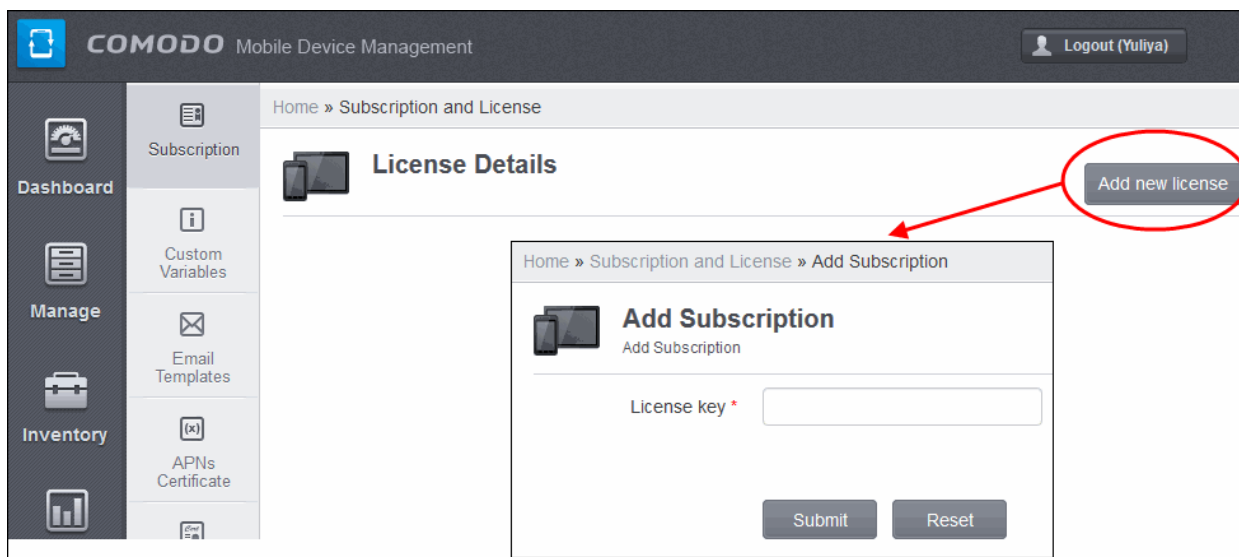
- Log in at <https://accounts.comodo.com> with your Comodo username and password
- Select 'Comodo Mobile Device Manager' and complete the purchase process.

Your license key will be sent via email to your registered email address.

Once you have obtained a new license, you need to register it in the interface.

### To add a new license

- Open the 'Subscription and License' panel by clicking the 'Settings' tab and choosing 'Subscription'.
- Click the 'Add new license' button at the top right.



- Enter the license keys from your license confirmation email.
- Click 'Submit'. Your new license will be activated.
- The license key will be displayed in the 'Subscription and license' panel
- To view the license details and activation status, click the arrow button next to license key.

Home » Subscription and License

**License Details** Add new license

209a4f55-e64b-49f1-aca0-d5406d9c8784 (support)  
Will expire in 164 day(s)

Subscription ID	880e1310d#
License key	209a4f55-e64b-49f1-aca0-d5406d9c8784
Max. Users	99
Organization	
Licensed to	Yadym Yikensky
Free	No
Active	Yes
Valid From	2014-01-30T13:26:29+04:00
Expires	2015-01-30T13:26:29+04:00
Time check	2014-08-18T10:14:43+04:00
License Registered at	2014-03-13T15:51:31+04:00

### New License

Please ensure to validate your license within 10 days after registration and starting using CMDM, else access to CMDM will be blocked.

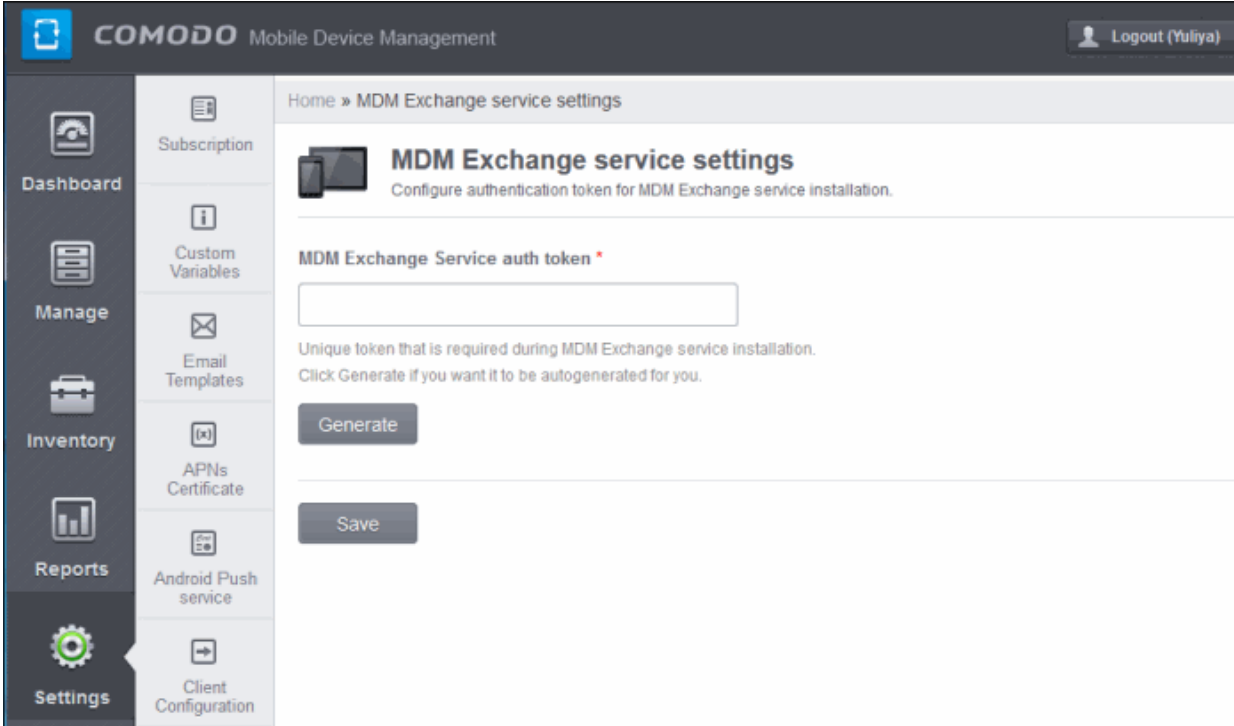
### Renewal

Make sure to renew your license before expiry and activate it. If the license is not renewed, admins will have access to the MDM portal for 30 days only after the expiry of the license. After this grace period, access to the CMDM will be blocked.

## 7.11. Generating MDM Exchange Service Token

The 'MDM Exchange Service settings' pane allows administrators to generate a unique token that is required during the MDM Exchange service installation. Refer to the next section '[Installing Exchange Service](#)' for more details.

To open the MDM Exchange Service settings interface, click the 'Settings' tab from the left hand side navigation and choose 'Exchange Settings' from the options.




The screenshot shows the Comodo Mobile Device Management interface. The top navigation bar includes the Comodo logo and the text 'Mobile Device Management', along with a 'Logout (Yuliya)' button. A sidebar on the left contains icons for 'Dashboard', 'Manage', 'Inventory', 'Reports', and 'Settings'. The main content area is titled 'Home » MDM Exchange service settings'. Below this, there is a section for 'MDM Exchange service settings' with the subtitle 'Configure authentication token for MDM Exchange service installation.' A form labeled 'MDM Exchange Service auth token \*' contains an empty input field. Below the field, there is a 'Generate' button and a 'Save' button. Text below the field explains that the token is unique and required for installation, and that clicking 'Generate' will autogenerate it.

To generate a unique authentication token, click 'Generate' and then the 'Save' button. This MDM Exchange Service auth token should be used during the Exchange service installation to establish connection between the Exchange server and CMDM server.

**Note:** If you generate a new token and save, then the connectivity between the Exchanger server and CMDM server will be lost. To reestablish connection again, the new token should be entered in the MDM Exchange service.

### 7.11.1. Installing Exchange Service

The CMDM Exchange Service should be installed on the Exchange server that you want to connect to the CMDM server. After downloading the setup file transfer it to the Exchange server and double click it.

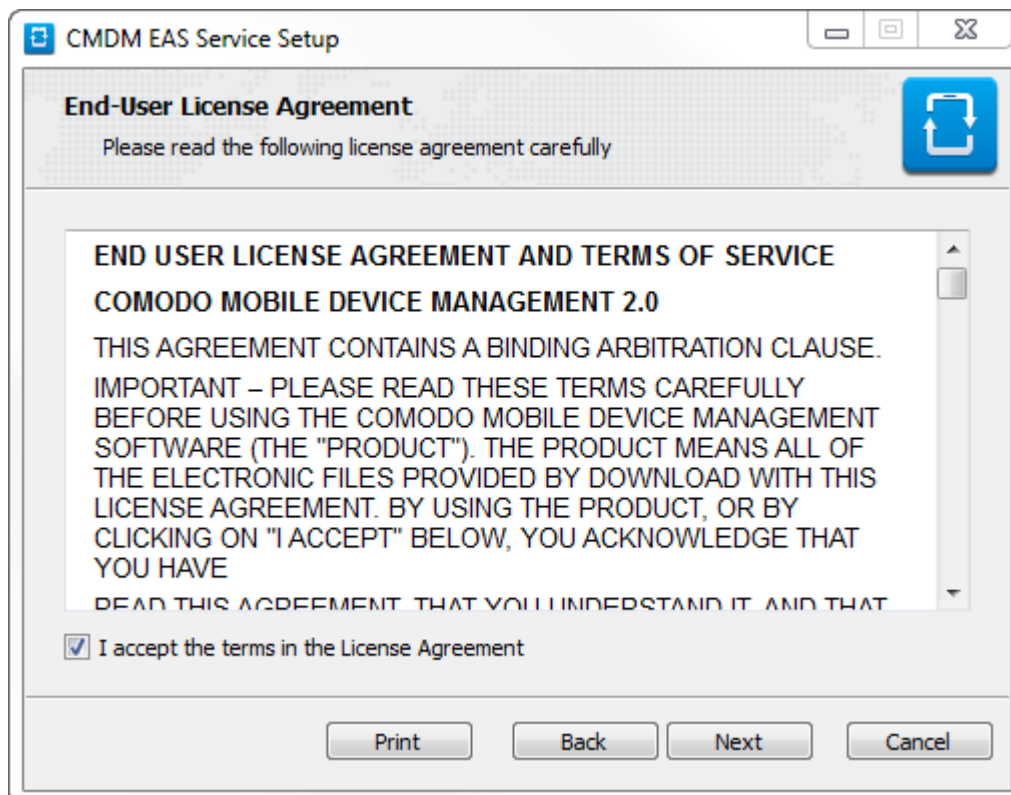
- Open the CMDM EAS service setup file  and select 'Run'.

The CMDM EAS Service setup wizard will start:

- Click Next

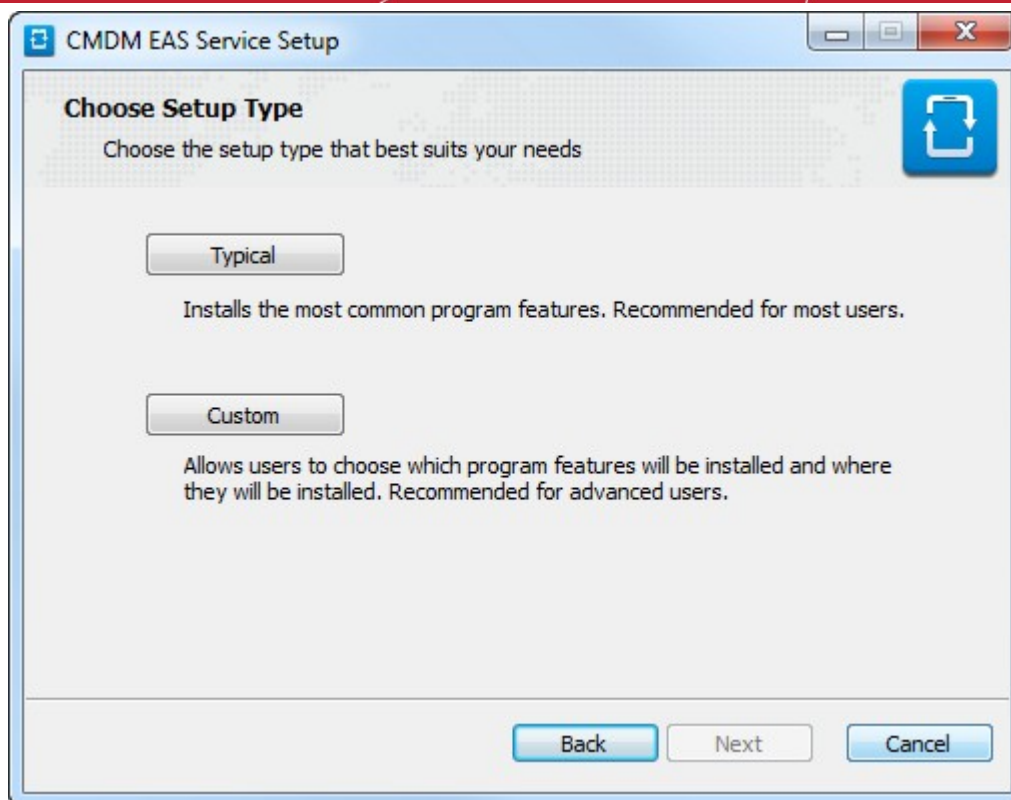


- Read and accept the End User License Agreement (EULA) and click Next.

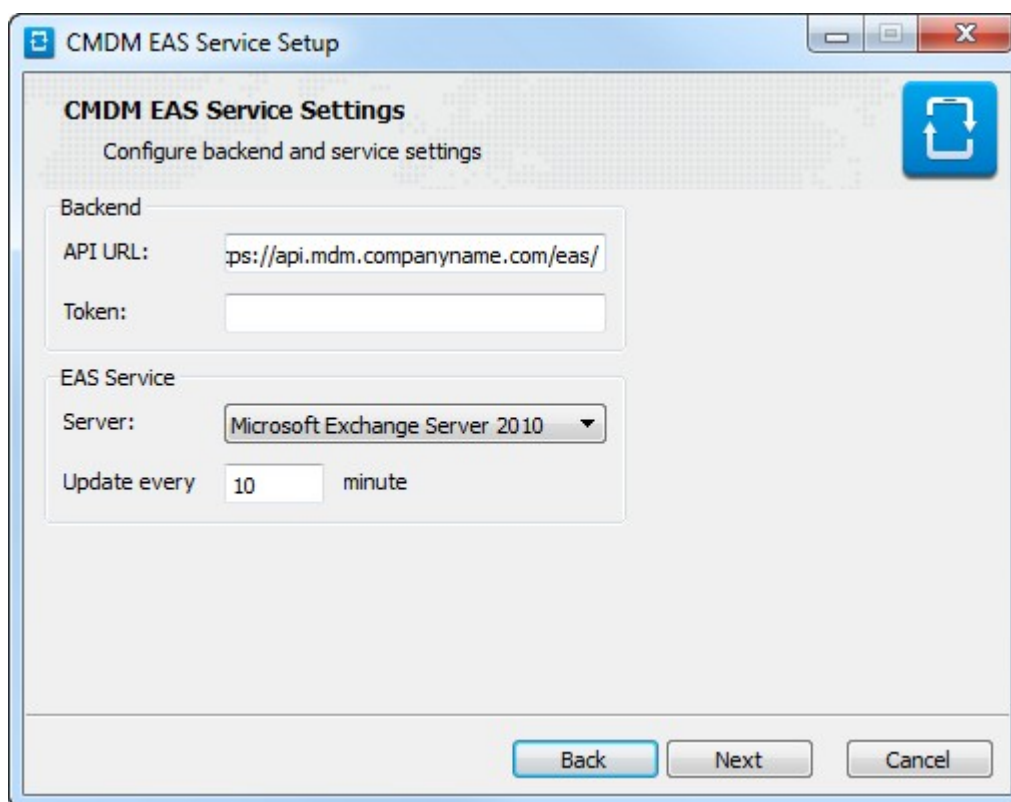


- Choose setup type to be installed.





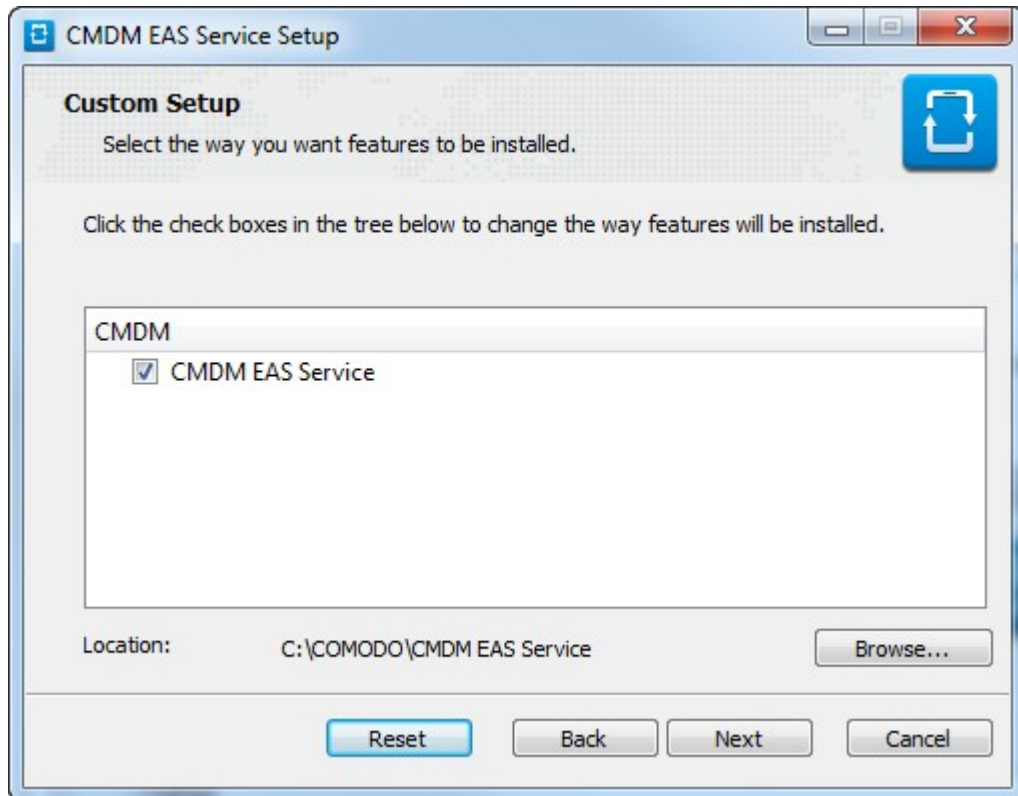
- **Typical** – Installs all components, CMDM backend and EAS Service to the default location C:/Comodo > CMDM



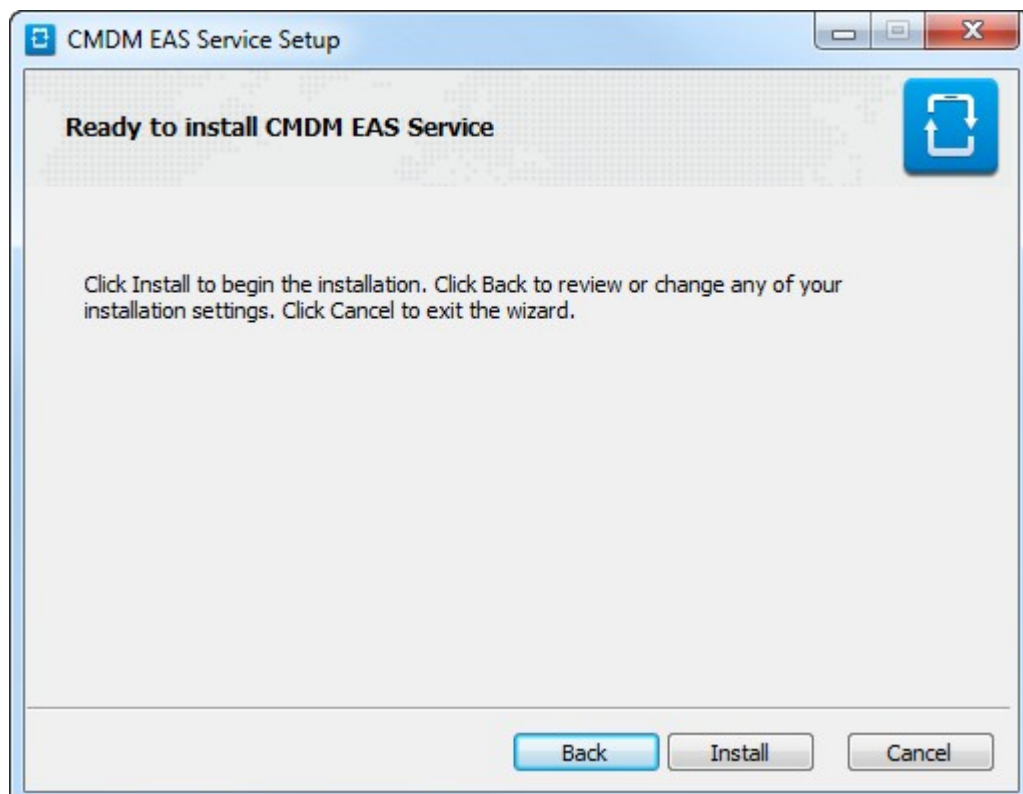
- API URL - Enter the URL that will host the CMDM backend.
- Token – Enter the generated unique token. Refer to **Generating MDM Exchange Service Token** section for more details.
- Select the type of Exchange Server from the Server drop-down.



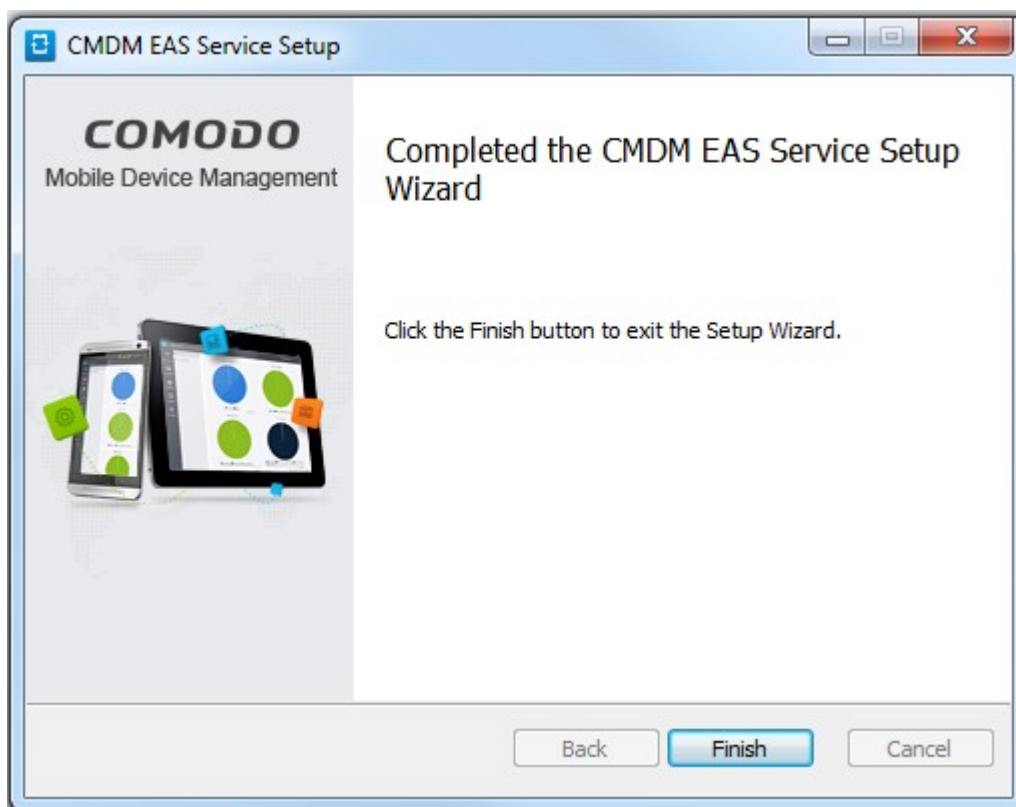
- Enter the time period in 'Update period' field at which info about all new added devices will be updated. By default this period is 10 minutes.
- Click 'Next'.
- **Custom** – Enables you to choose which components are installed and to modify the installation path if required.



- Installation proper will commence after you click the 'Install' button. Use the back button if you wish to review your installation settings.



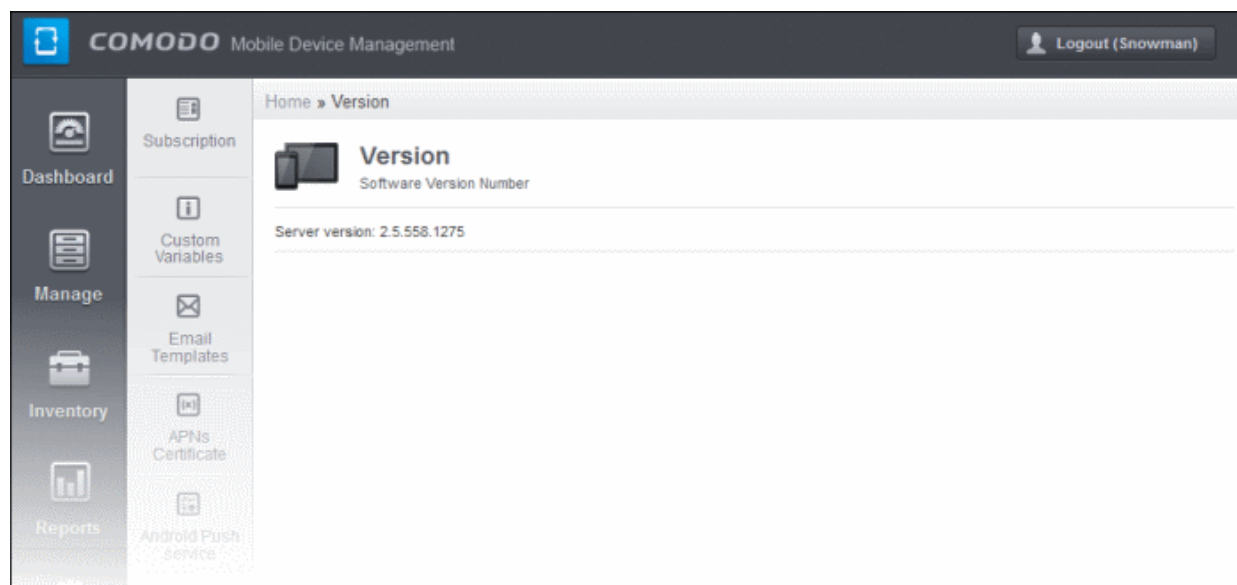
- After setup is complete, click 'Finish' to finalize installation and exit the wizard



## 7.12. Viewing Version Information

The Version information pane displays the version number of Comodo Mobile Device Manager's application.

To open the 'Version' panel, click the 'Settings' tab from the left hand side and choose 'Version'.



## About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

### **Comodo Security Solutions, Inc.**

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)

For additional information on Comodo - visit <http://www.comodo.com>.