COMODO
Creating Trust Online®

Comodo
Mobile Device Manager

Software Version 1.0

Quick Start Guide

Guide Version 1.0.030314

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ 07013

Comodo Mobile Device Manager - Quick Start

This tutorial explains how to use Comodo Mobile Device Manager (CMDM) to add users, enroll devices, create device groups and create/deploy device configuration profiles:

Note – this guide assumes you have already successfully completed all steps in the CMDM installation guide - including activating your license and acquiring an Apple Push Notification certificate.

If you have not yet done so, please see **http://help.comodo.com/topic-214-1-524-6411-CMDM-Setup.html**

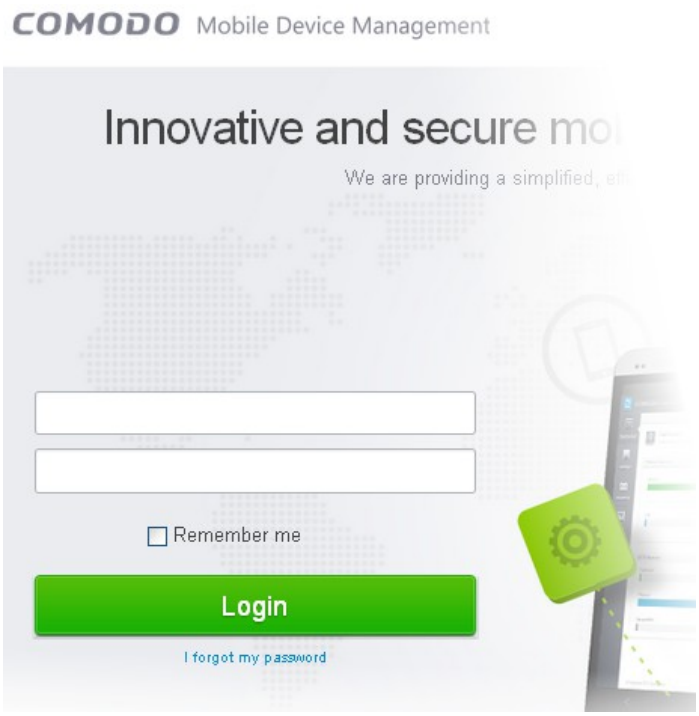
Step 1 - Login to the Admin Console

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

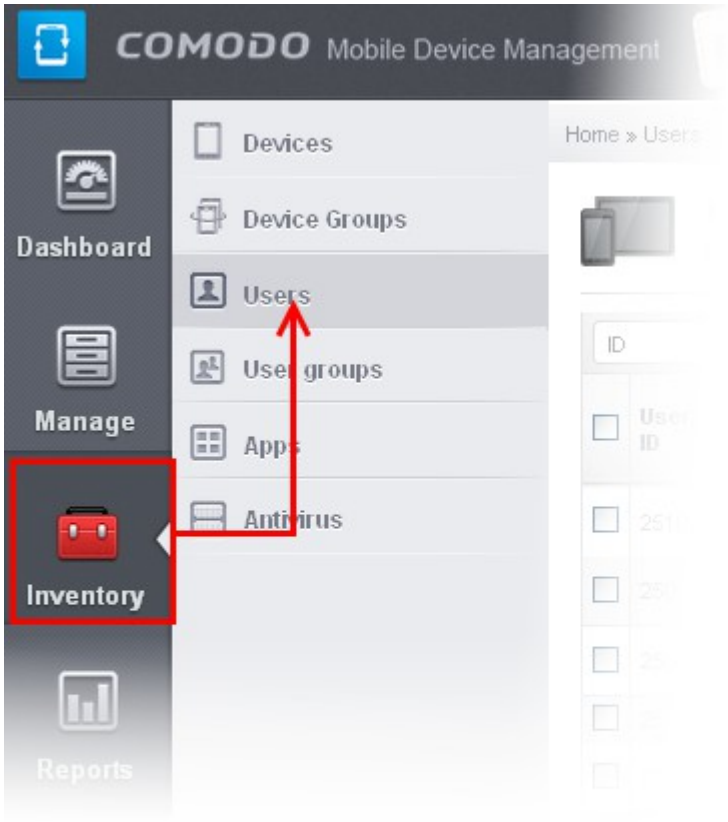


You can (and should) change these to a unique username and strong password. To do this, log in, click 'Inventory' > 'Users' then click on the user named 'Admin'. Next, click the 'Update' link. The 'Update User' screen will allow you to change your username and to initiate the reset password process.

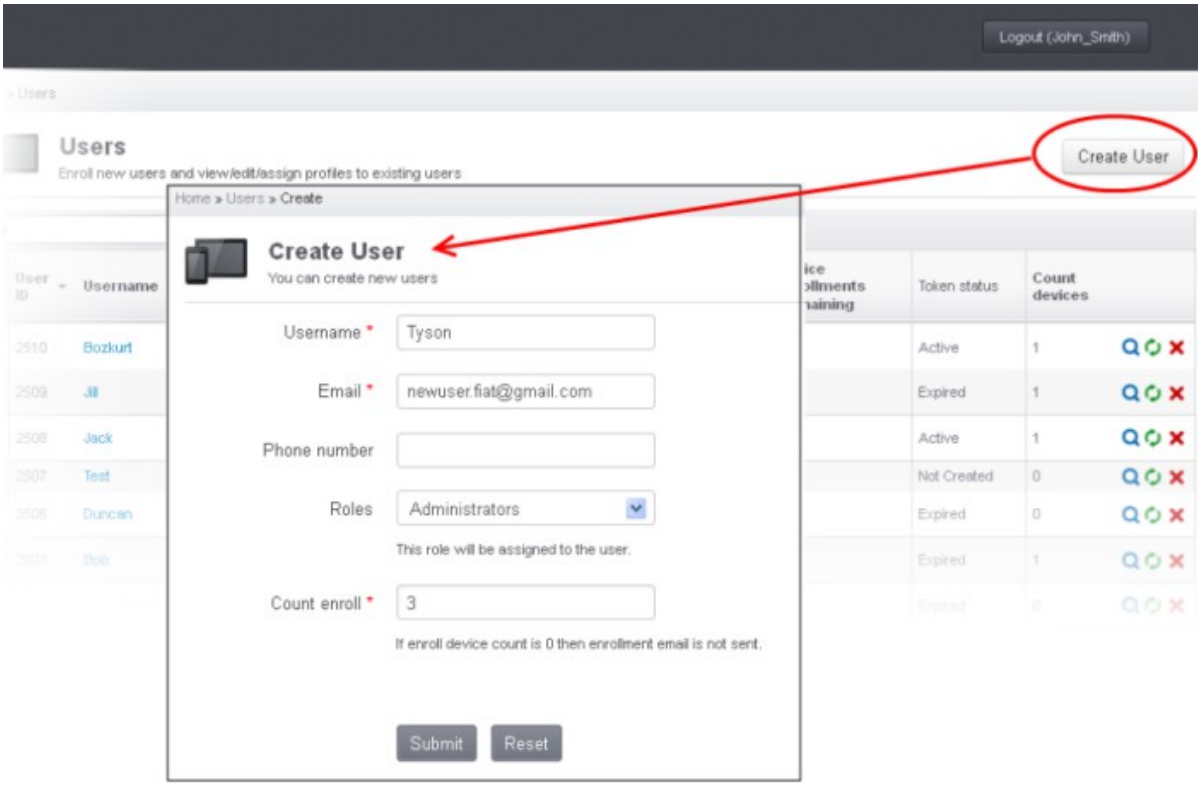
Step 2 – Add Users and Enroll devices

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

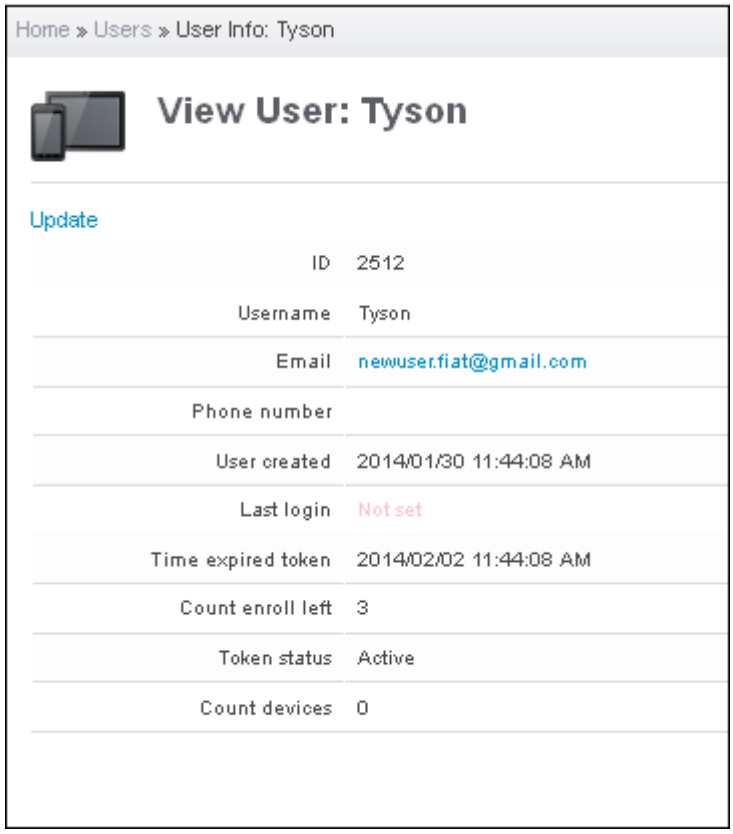


- Click the 'Inventory' button on the left and choose 'Users'



- Next, click 'Create User' at the top right of the 'Users' interface:
- Type a login username (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 default 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.



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.

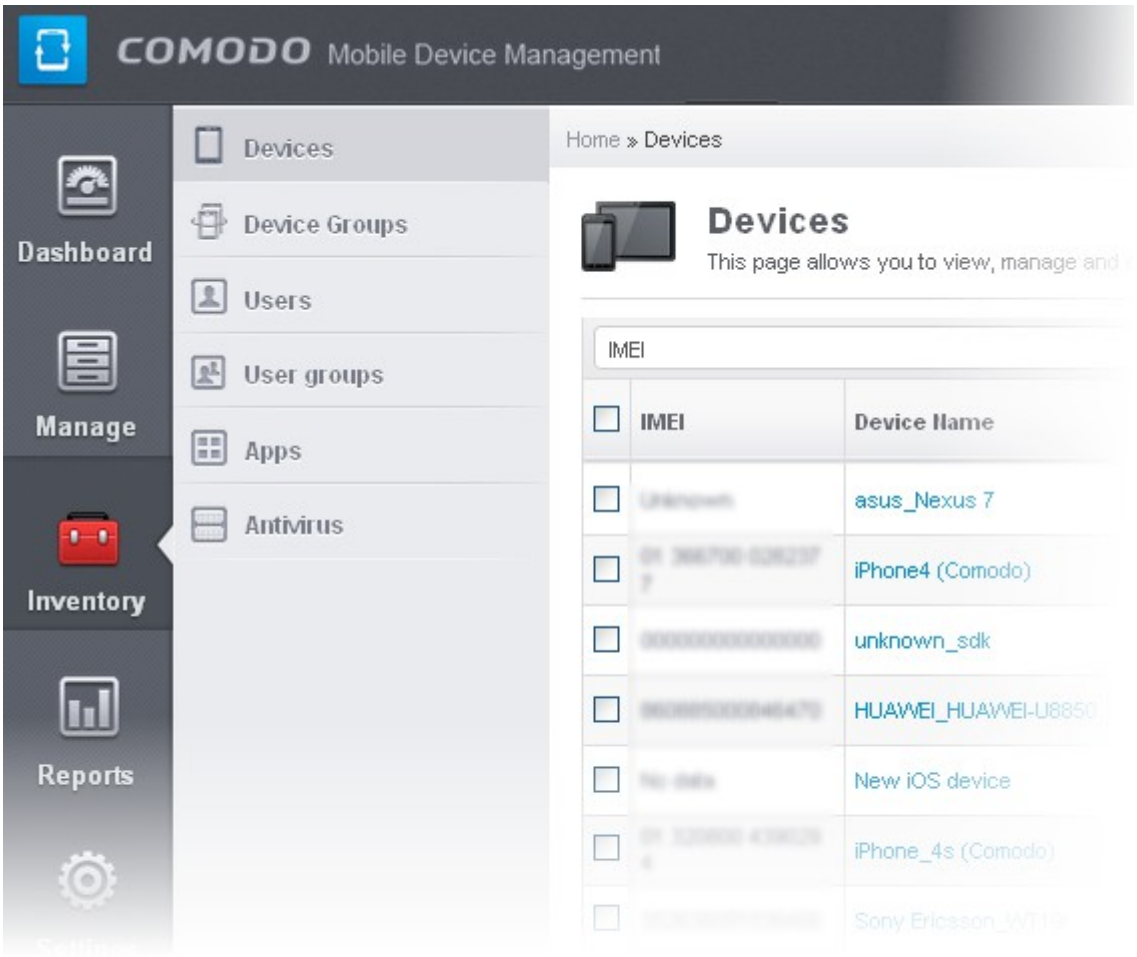
Enroll iPhones, iPods and iPads

The device enrollment email contains two links. The first is to download the CMDM client authentication certificate. 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. The second link in the mail is to download the device configuration profile and so enroll the device.

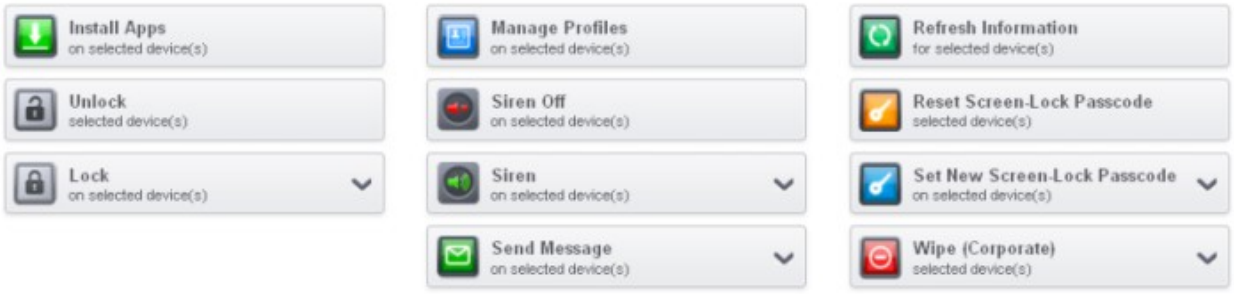
Note: The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

1. User receives enrollment mail, opens certificate download link then installs the certificate on their device.
2. After certificate installation, the user opens the enrollment link in the mail. The device configuration profile will be downloaded and installed. 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 (optional)

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 group' button or the 'Create iOS group' button.
- The 'Admin device group' interface will open. You now have to name the group and choose which devices you wish to add.
- Devices which are eligible for the group are displayed in the left-hand pane. The right-hand pane will display devices that have been added to the group. Select a device from the left and click the ' >> ' button to add it to the group (use the CTRL or Shift keys to select multiple devices).
- Profiles are **explained in the next section**.
- Click 'Save'. Repeat the process to create more groups.

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.

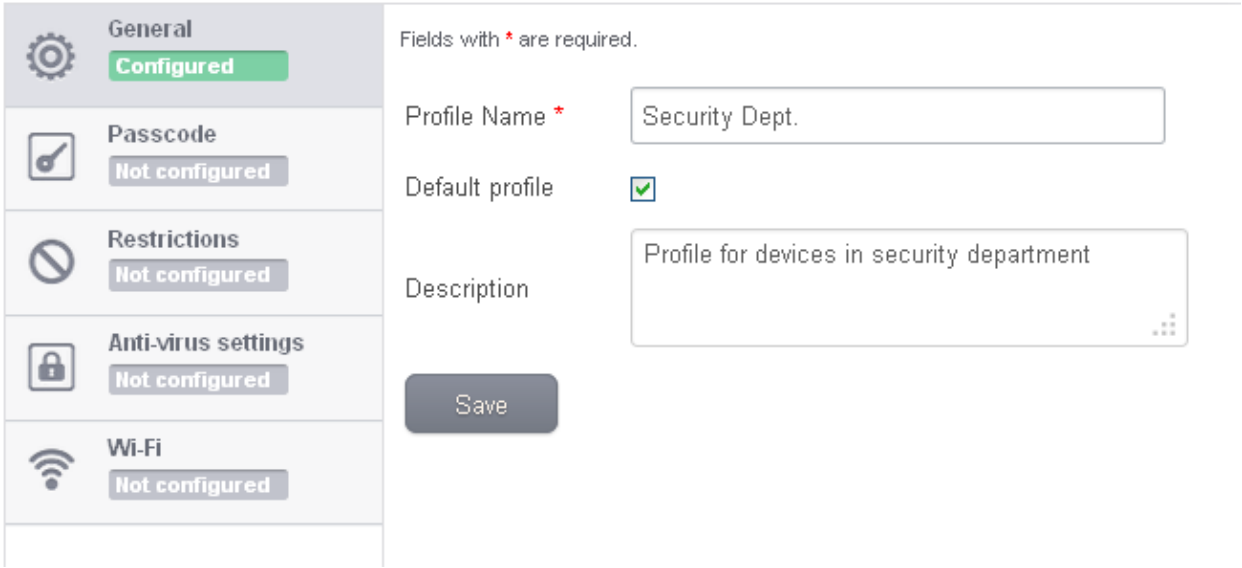
Profile specification differs slightly between iOS and Android:

Android profiles

iOS profiles

To create an Android Profile

- 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'.



Android profile configuration screen

After saving, you will move onto profile configuration where you can configure passcode settings, feature restrictions, antivirus settings and Wi-Fi settings. 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'.

To create an iOS Profile

- 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 poxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.

Cellulars – Configure cellular network settings. The 'cellulars' setting performs fulfills 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 the '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

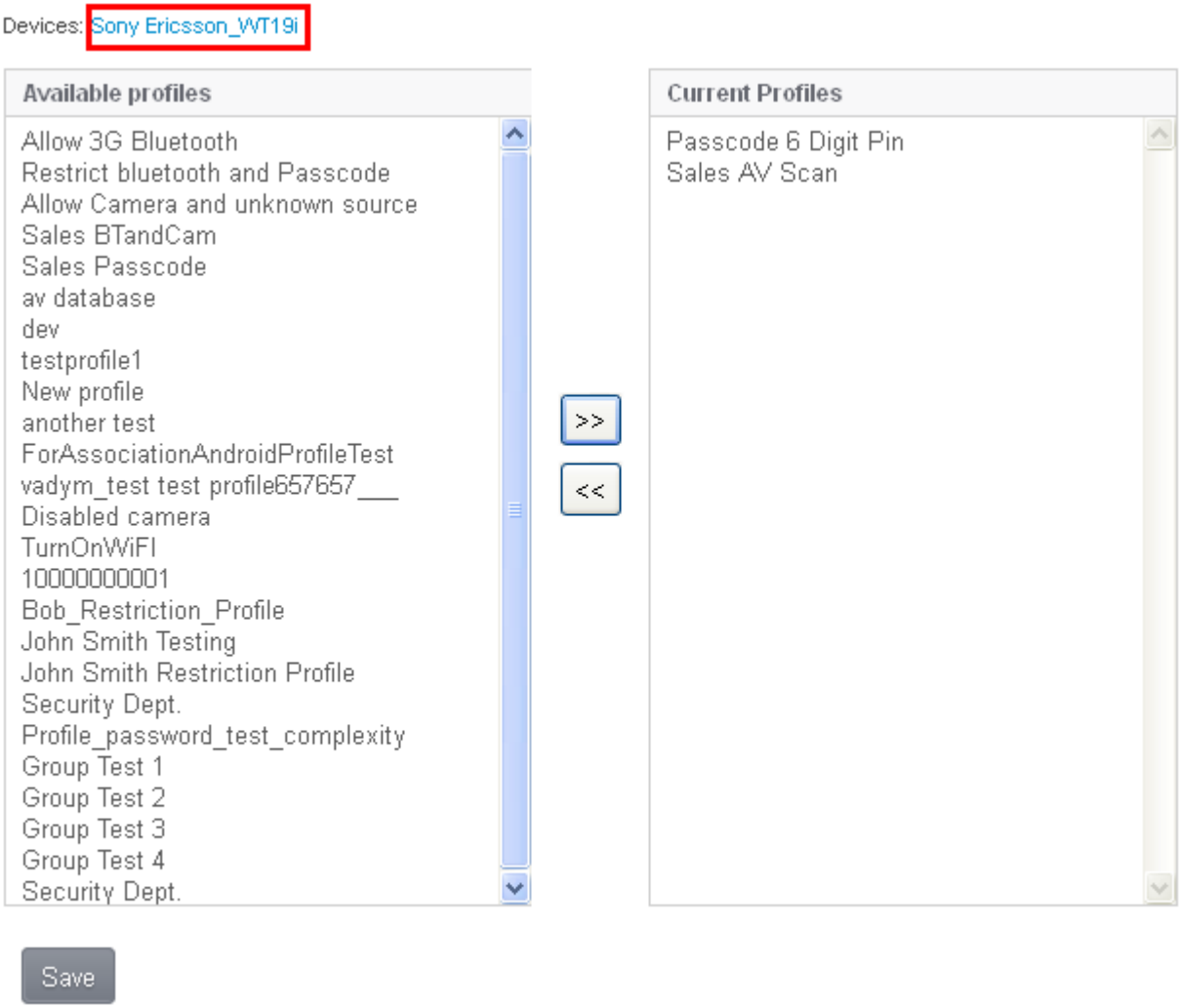
1. Click 'Inventory' > 'Devices', to open full list of currently enrolled devices.
2. Select the device(s) to which you wish to apply a profile or profile group. Make sure all devices are of the same

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.

5 Use the drop down to select whether you want to apply individual profiles or a (previously created) profile group.



- To add a profile/profile group to the chosen device(s), select the profile from the left and click the '>>' button. Use Shift or CTRL keys to select multiple profiles at once.
- 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 or profile group 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**

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

STE 100

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.