COMODO
Creating Trust Online®

Comodo
Device Manager

Software Version 4.0

End User Guide

Guide Version 4.0.112316

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo Device Manager 3
2.Enrolling Your Membership 3
3.Enrolling Your Device 4
3.1.Enrolling Android Devices 4
3.2.Enrolling iOS Devices 13
3.3.Downloading and Installing CDM Client for iOS Devices 15
3.4.Enrolling Windows Endpoints 19
4.Logging-in to CDM Console 22
5.The Administrative Console 23
5.1.The Dashboard 23
5.2.Viewing Version Information 25
About Comodo 27

1.Introduction to Comodo Device Manager

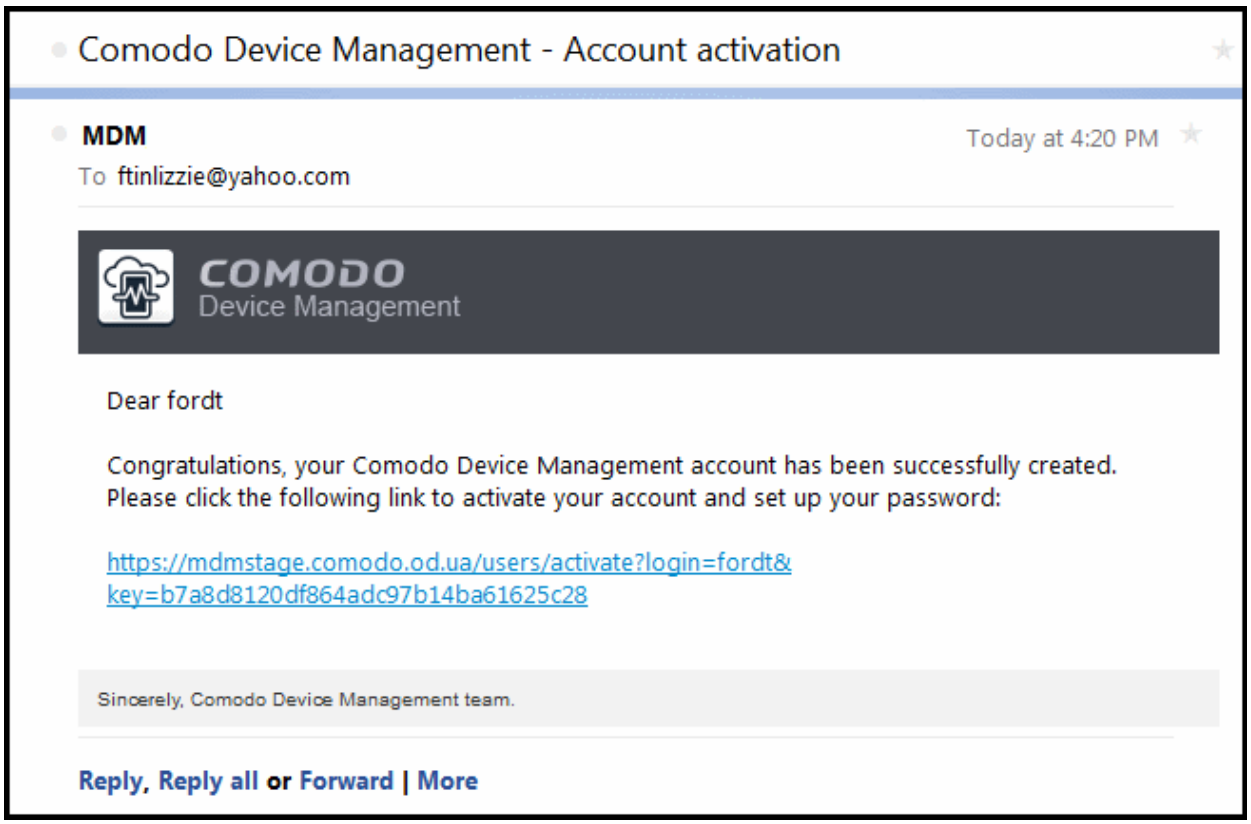
Comodo Device Manager (CDM) is a centralized device management system that allows network administrators to manage, monitor and secure mobile devices which connect to enterprise networks. Once you have enrolled your Android, iOS or Windows device, it will have a security policy applied to it which will authenticate it to your company network and protect it from malware.

This guide explains the steps to enroll your device, login to the Comodo Device Manager user interface and how to view reports. If given appropriate privileges, you may be able to control some other aspects of your device too.

- **Enrolling your Membership**
- **Enrolling your Device**
  - **Android Devices**
  - **iOS Devices**
  - **Windows Devices**
- **Logging-in to CDM console**
- **The Administrative Console**
  - **The Dashboard**
  - **Viewing the Version Information**

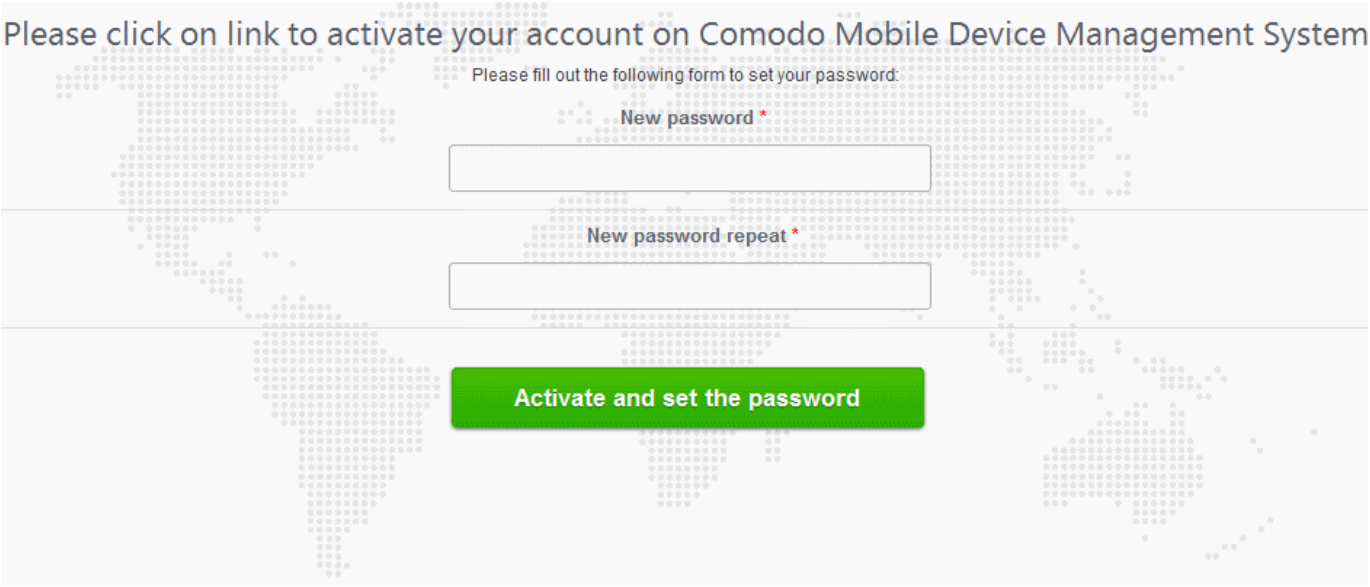
2.Enrolling Your Membership

In order for your device(s) to be enrolled to CDM, an user account should be created for you at the CDM by the administrator. Once the administrator adds you as a user to CDM, you will receive an activation mail at your registered email address. You need to activate your account by clicking the activation link in the mail and setting a password. An example mail is shown below.



- Click the activation link in the email.

You will be taken to the account activation page.



- Enter a new password for your account and re-enter it for confirmation in the respective text fields.
- Click the 'Activate and set the password' button.

Your account will be activated and you will be taken to the login page of CDM. See the section **Logging-in to CDM console** for more details.

The administrator can now add your devices to be enrolled.

3. Enrolling Your Device

Once the administrator adds your device(s) for enrollment, you will receive a device enrollment procedure mail at your registered email address. You can download/install the iOS profiles, Android Agent and/or Windows agent and configure them by clicking the appropriate links in the device enrollment mail. You can use the same enrollment email to enroll different devices of number specified for your user account by the administrator.

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

- **Enrolling Android Devices**
- **Enrolling iOS Devices**
- **Downloading and Installing CDM Client for iOS Devices**
- **Enrolling Windows Endpoints**

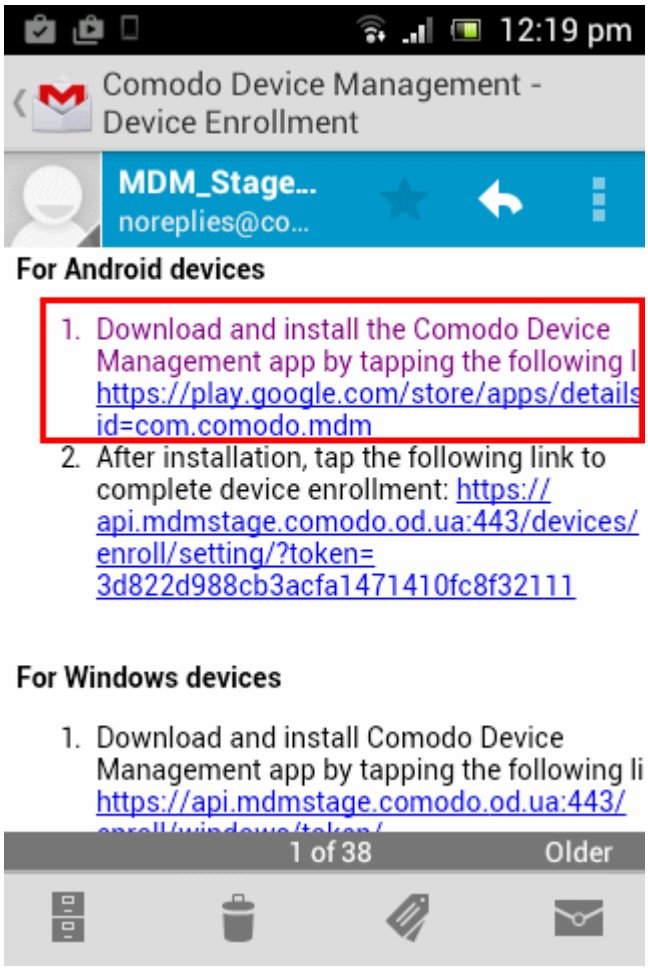
3.1. Enrolling Android Devices

The enrollment email contains a link to download the android CDM agent and a link to configure the agent. The email will also contain instructions to 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.

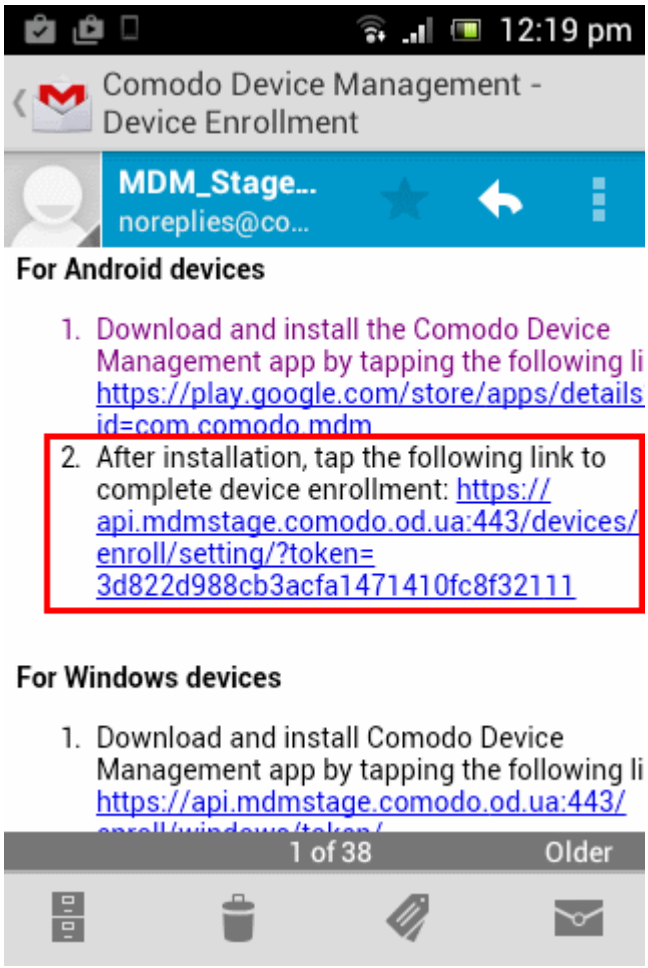
Step 2 - Configuring the agent

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

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

Automatic Configuration

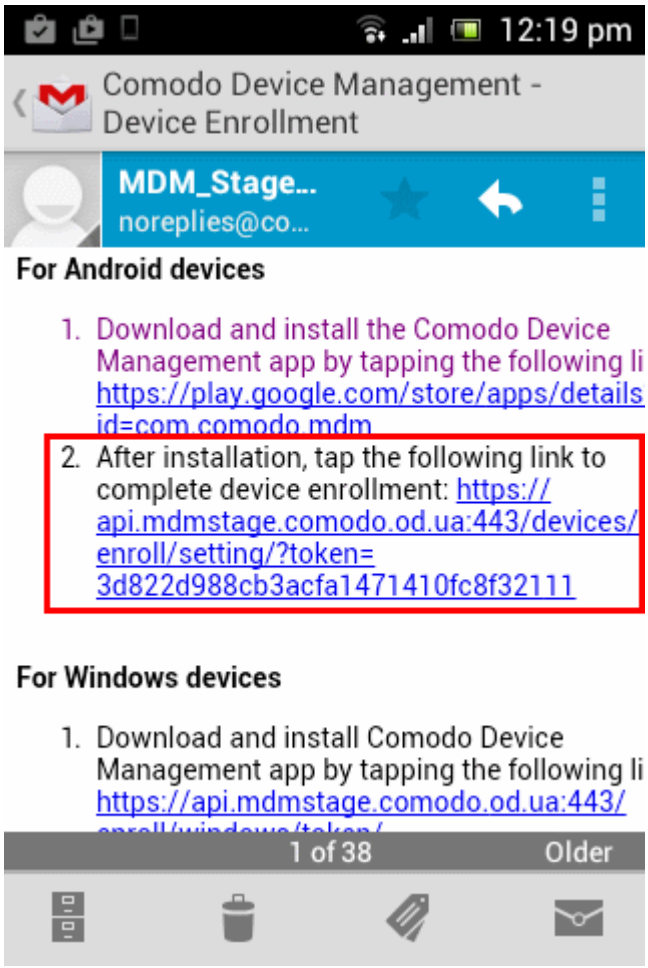
- Tap the enrollment link contained in the email after the completion of installation.



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

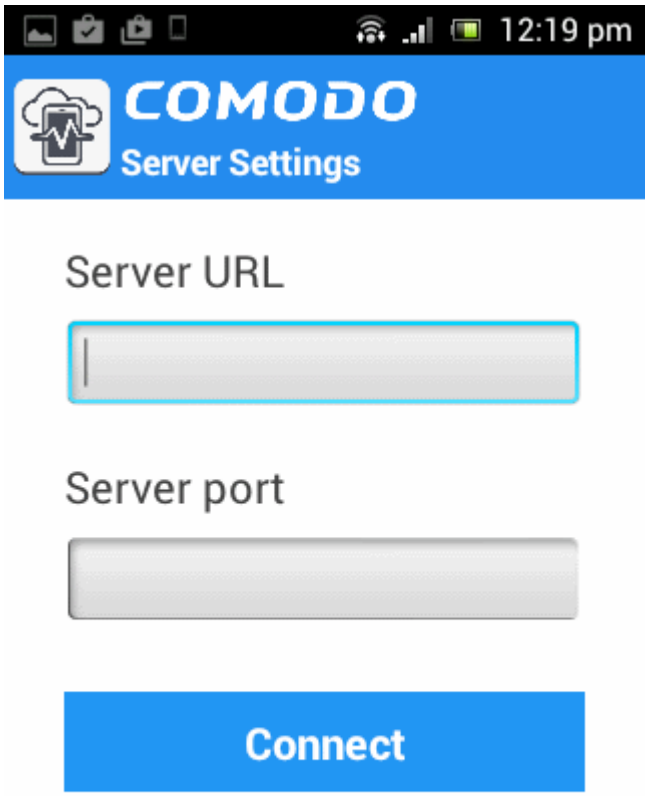
Manual Configuration

You can manually configure the agent to connect to CDM server by entering the server settings and the token ID contained in the enrollment email.



- 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 CDM server contained in the mail.
Server port	Text Field	Enter the connection port of the server for your device to connect, as specified in the mail. (Default = 443)

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

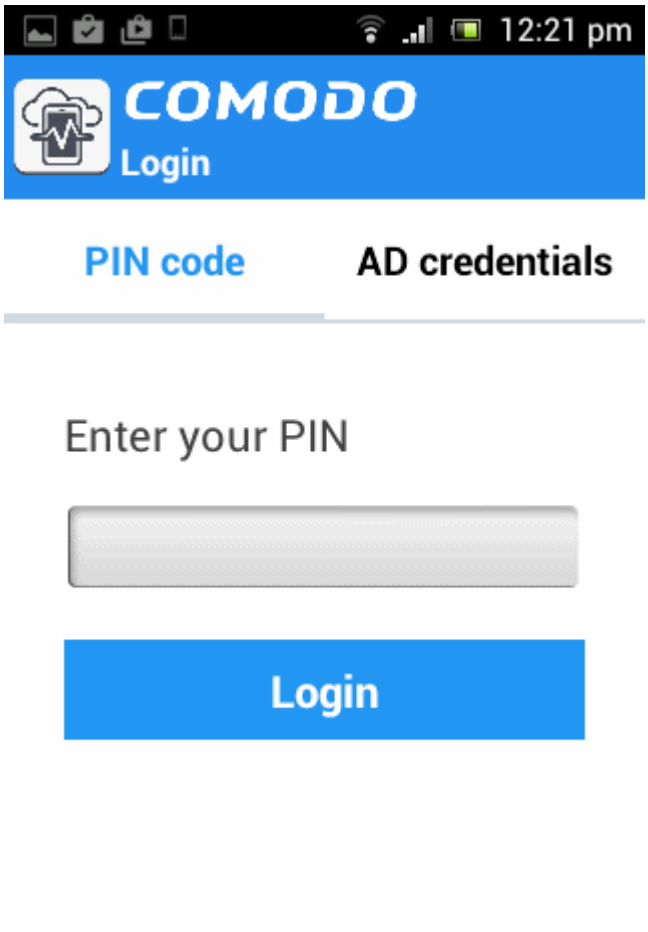
Logging-in to the Console

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

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

Entering PIN

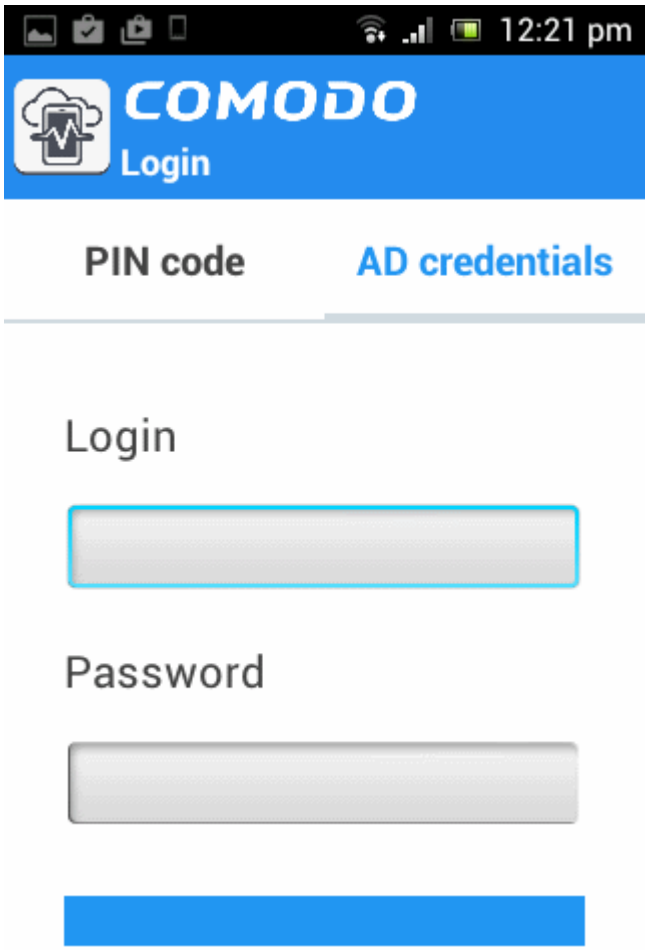
- Tap the '**Pin Code**' tab in the 'Login' screen



- Enter the PIN (token) contained in the enrollment email
- Tap 'Login'. The **End User License Agreement** screen will appear.

Entering your username and password

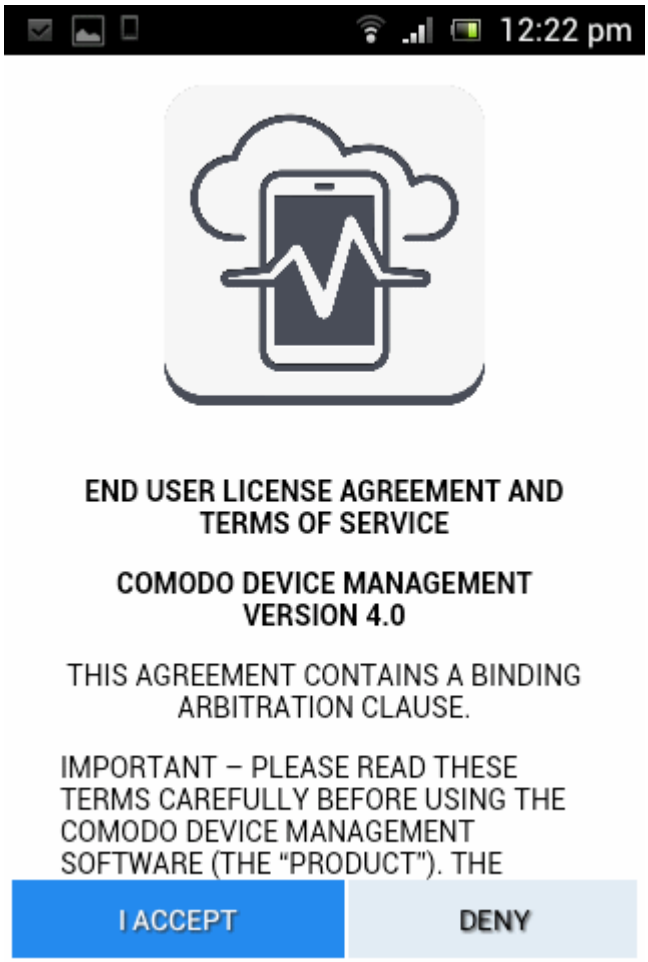
- Tap the '**AD Credentials**' tab in the 'Login' screen



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

End User License Agreement

The EULA screen will appear.

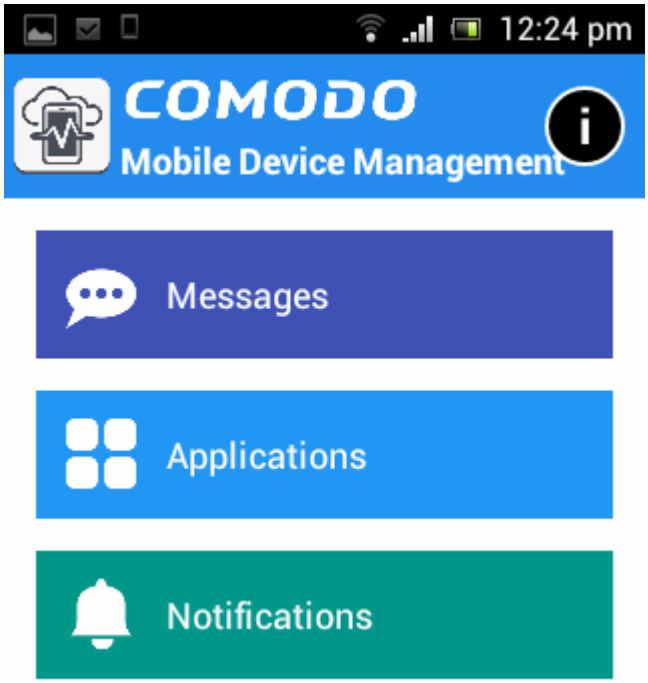


- Scroll down the screen, read the EULA fully and click the I Accept button at the bottom.

The Agent activation screen will appear.

- Tap 'Activate'.

The CDM agent home screen will appear.



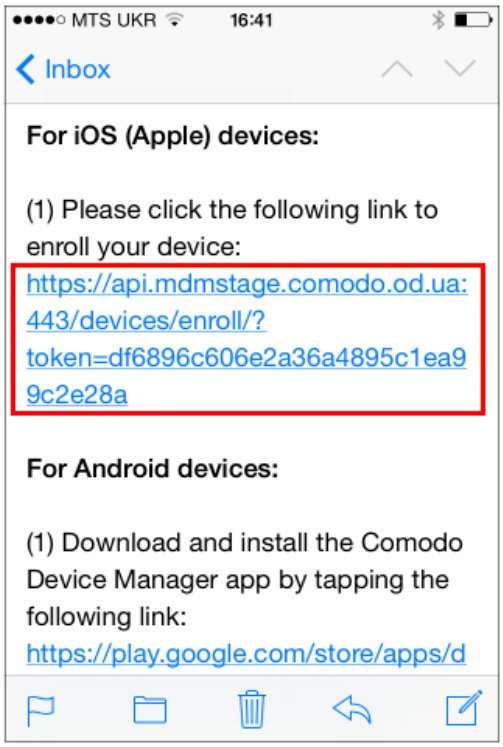
The device is enrolled to CDM and can be remotely managed from the CDM console.

3.2. Enrolling iOS Devices

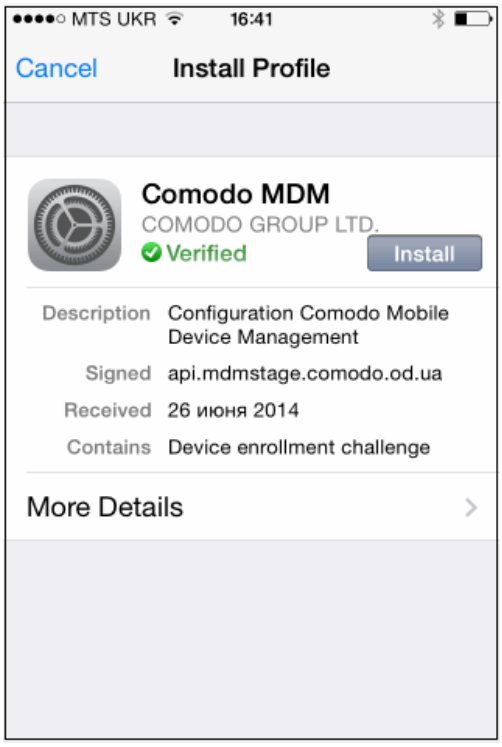
After the administrator has created a user, he / she will receive an enrollment email with the links to download the server certificate and the CDM profile. The user can follow the instructions in the mail and enroll the device in two steps.

Installing the Certificate

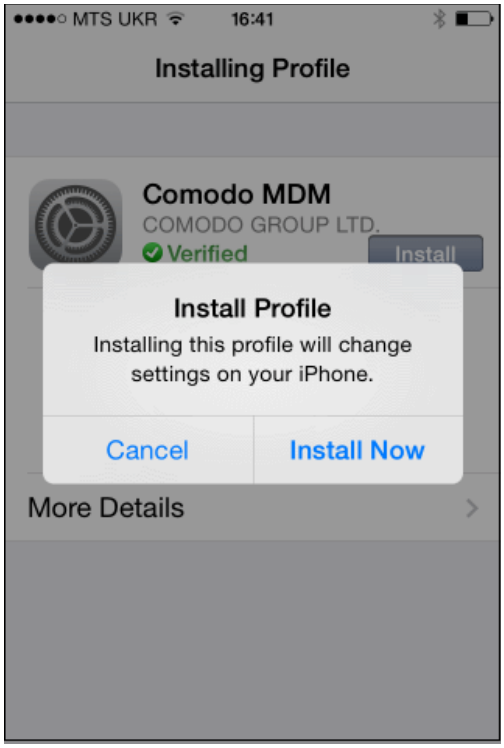
- Open the email on the device and tap the link under **For IOS only**



The 'Install Profile' wizard will start.

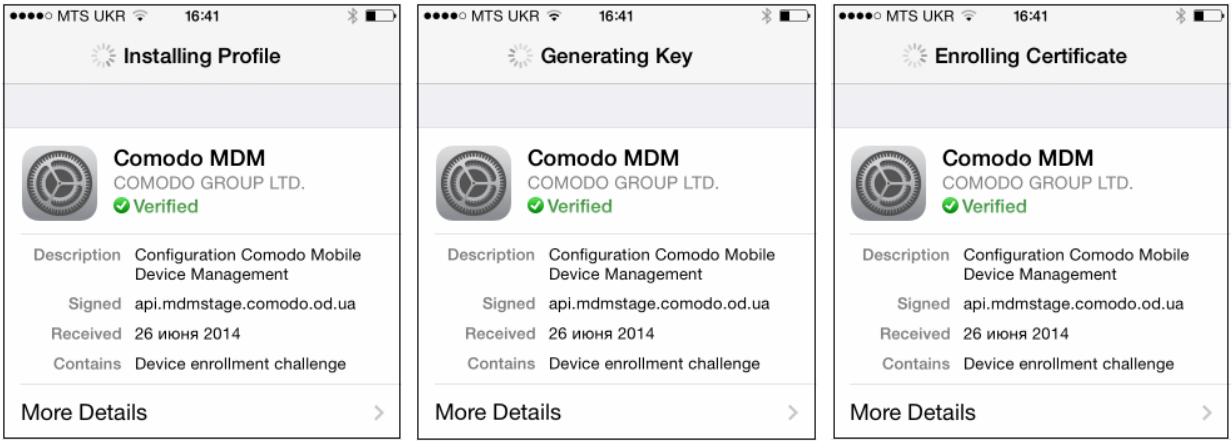


- Tap 'Install'. A confirmation dialog will be displayed.

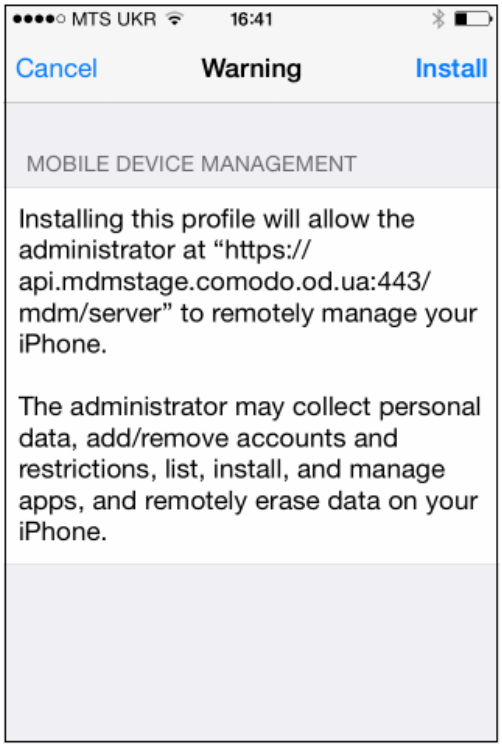


- Tap 'Install Now'.

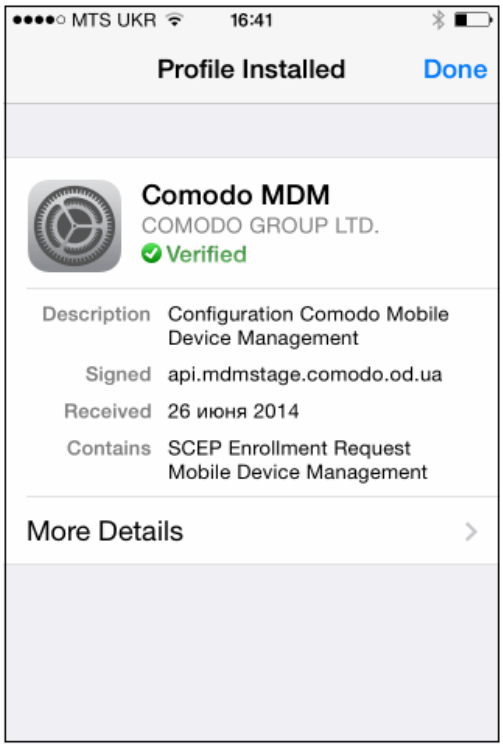
The CDM Profile installation progress will be displayed.



- 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.

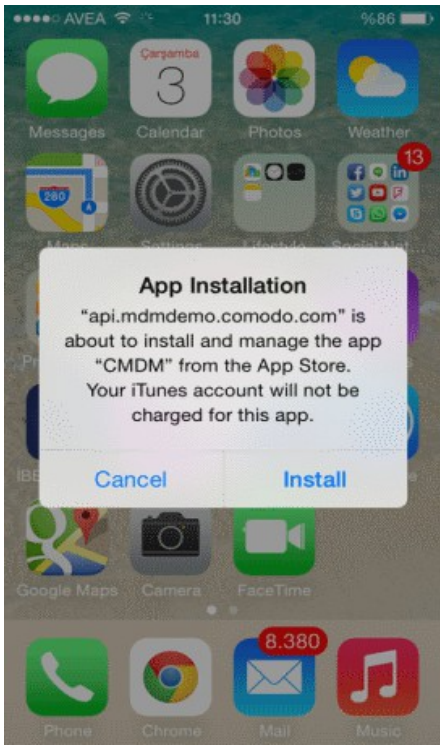
You can view the CDM profile listed in the profiles screen of the device.

3.3. Downloading and Installing CDM Client for iOS Devices

The iOS devices enrolled into CDM for management as explained in the previous section '**Enrolling iOS Devices**' do not support some features such as apps management, GPS location and messaging. To get full functionality, users need to download CDM client from iTunes website at **https://itunes.apple.com/us/app/cmdm/id807480077?mt=8**. CDM client supports iOS 6.0 and higher versions and is compatible with iPhone, iPad and iPod Touch.

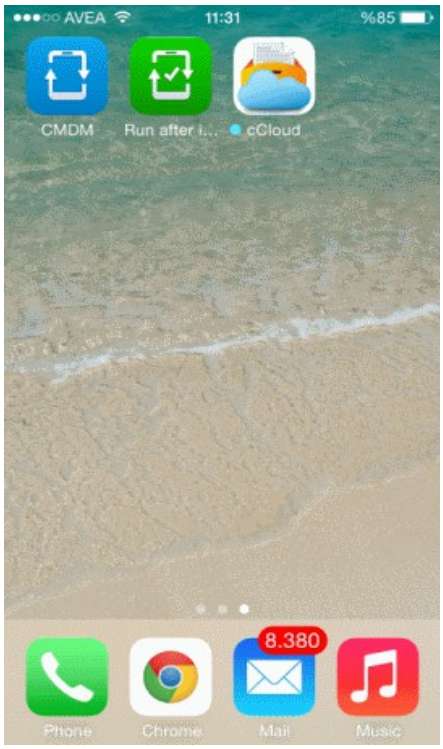
To download and install CDM client on iOS devices

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

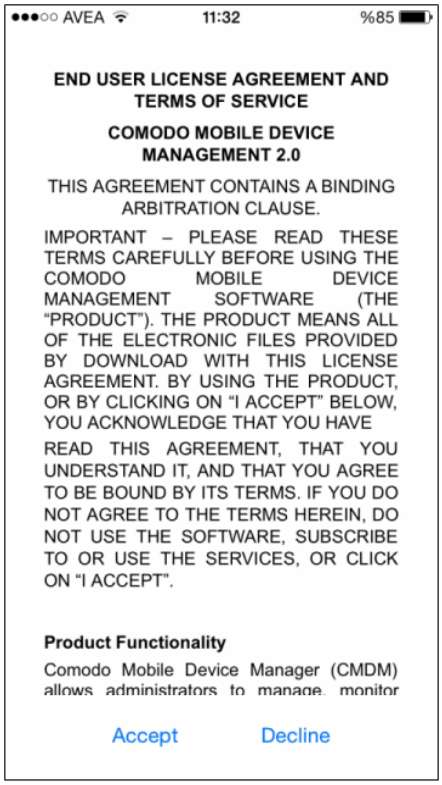


- Tap 'Install'

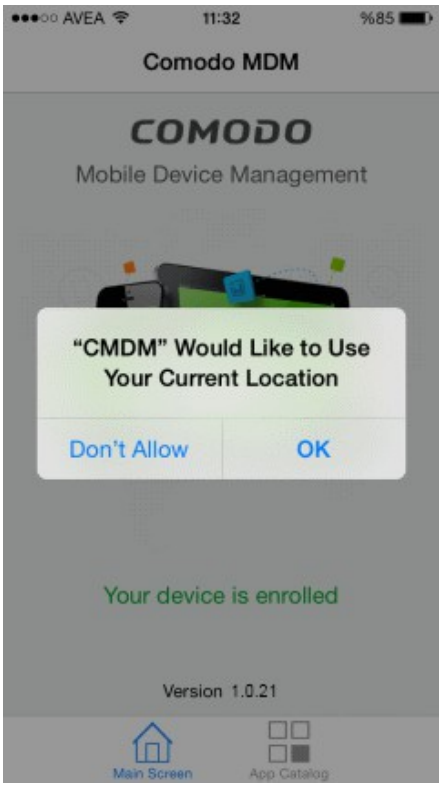
The CDM app will be downloaded and installed on the device.



- Tap on the CDM icon

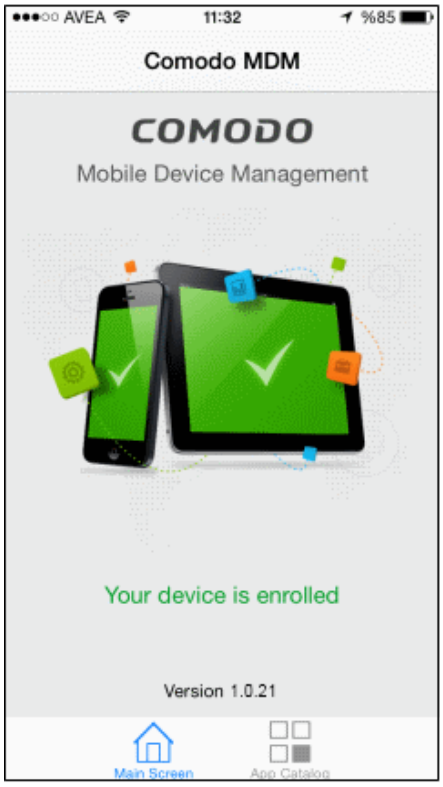


- Read the End User License Agreement fully and tap 'Accept'

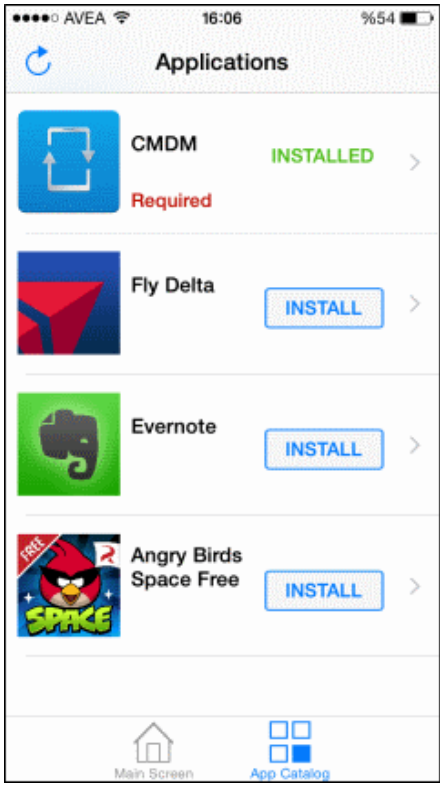


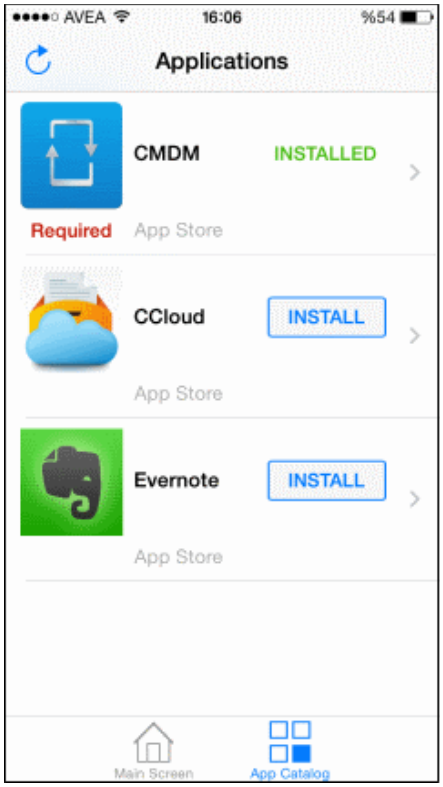
- Tap 'OK'.

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.



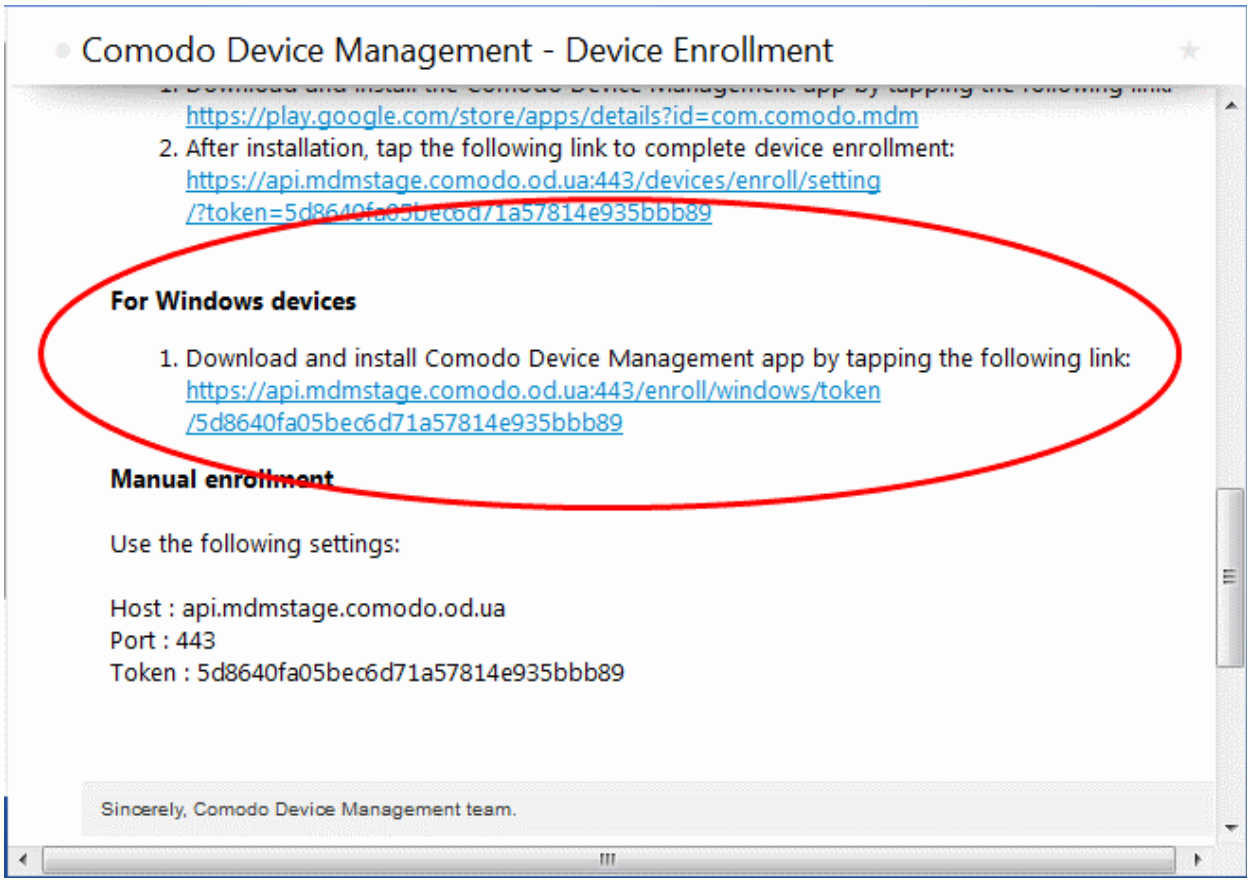


3.4. Enrolling Windows Endpoints

The enrollment email contains instructions and links to download the Windows CDM agent. You should open the email at the Windows endpoint to be enrolled and follow the instructions. Upon successful enrollment, the CDM agent will be installed on the endpoint and automatically configured to connect to the CDM server. Also, the endpoint security software 'Comodo Client Security (CCS)' will be installed with 'Sandbox', 'Antivirus' and 'Firewall' components as specified during device enrollment by the administrator.

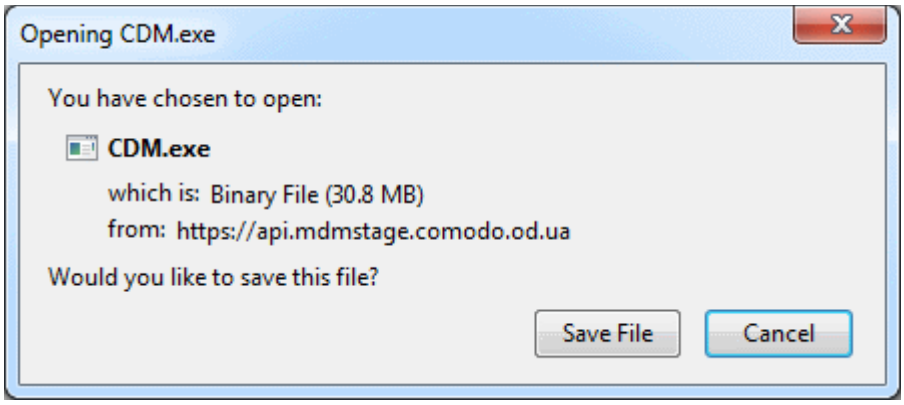
To enroll a Windows device

- Open the device enrollment email at the endpoint



- Click on the enrollment link under 'For Windows devices'.

The download dialog for the CDM agent setup file will appear.



- Download and save the setup file to the local drive
- Double click on the setup file and follow the installation wizard

On completion of installation, the device will be automatically enrolled o the CDM server.

Once the device is enrolled, the CDM agent will automatically download and install CES at the background. On completion of CES installation, the device will restart for the CES installation to take effect.

4.Logging-in to CDM Console

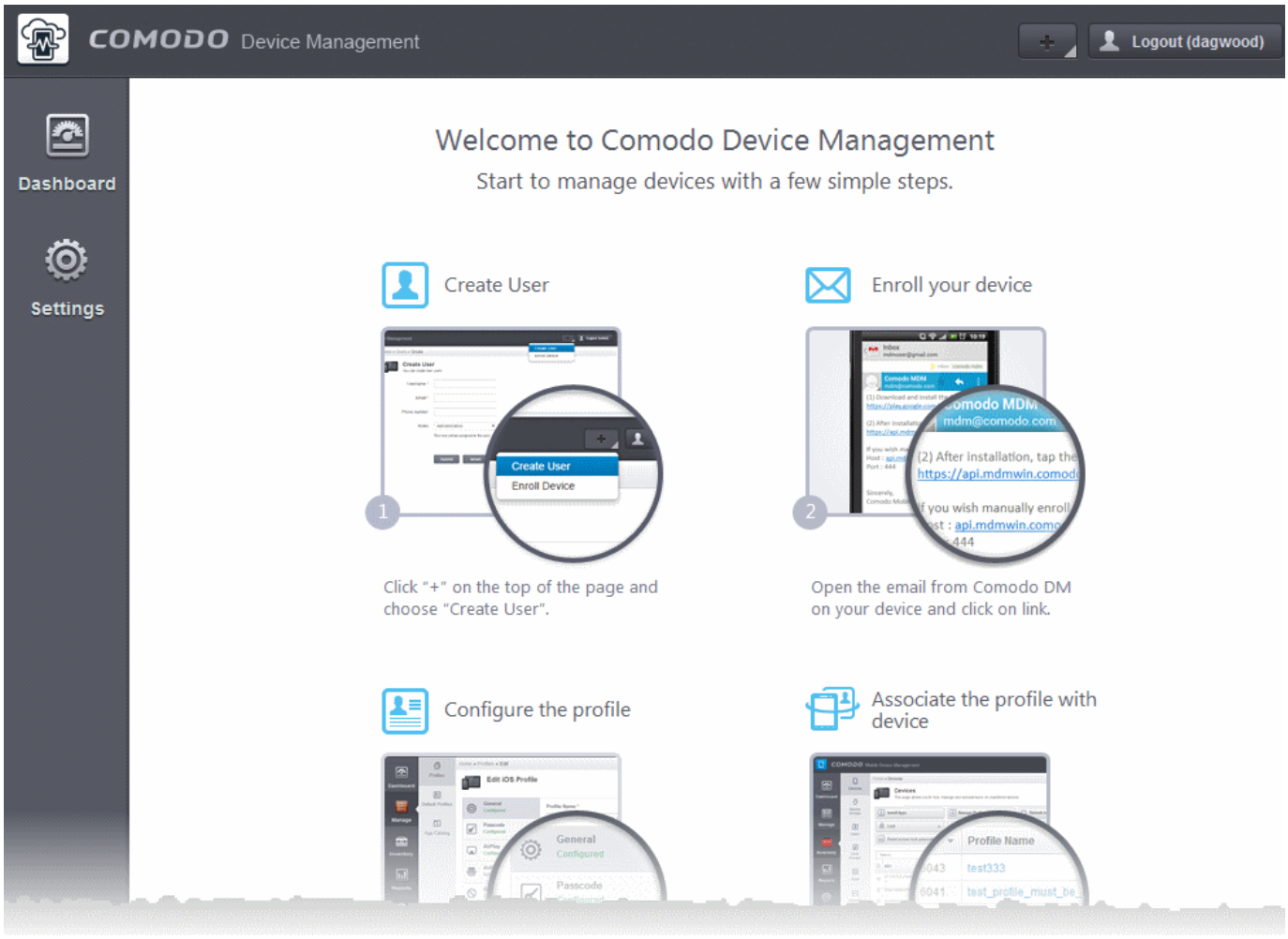
Once your account is activated, you can login to the web based CDM application using any Internet browser, by entering the URL of the CDM interface. Comodo Device Manager is a locally hosted solution. If you do not know the URL of the login page, then please contact your administrator.

- 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 Device Management' screen will be displayed.



Depending on the role configured for you, the interface allows to manage profiles, associate profiles with device and add users in a few steps. Refer to the Administrator Guide at **http://help.comodo.com/topic-214-1-519-6113-Introduction-to-Comodo-Device-Manager.html** for more details.

5. The Administrative Console

The Administrative Console allows the user to view the details of the devices enrolled to CDM.

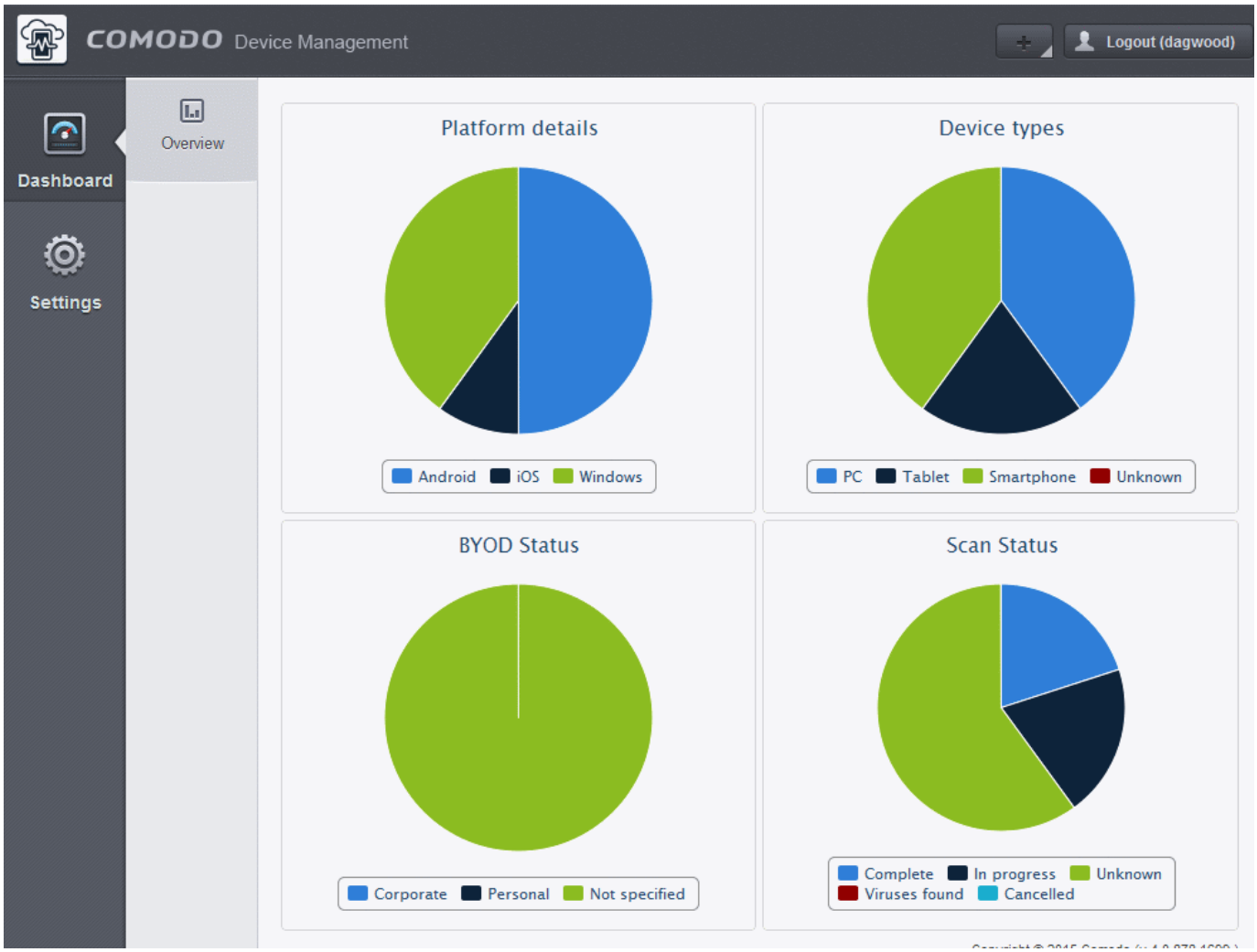
Once logged-in, you can navigate to different areas of the console by clicking the tabs at the left hand side. The number of tabs available at the left hand side depends on the role permissions configured for you. To know more about settings and configurations, refer to the Administrator guide at **http://help.comodo.com/topic-214-1-519-6113-Introduction-to-Comodo-Device-Manager.html**.

- **Dashboard** – Allows you to view snapshot summaries of details like operating systems, device types, AV scan status of devices enrolled to CDM as pie-charts. See **The Dashboard** for more details.
- **Settings** - Allows you to view the software version details. See **Viewing Version Information** for more details.

5.1. The Dashboard

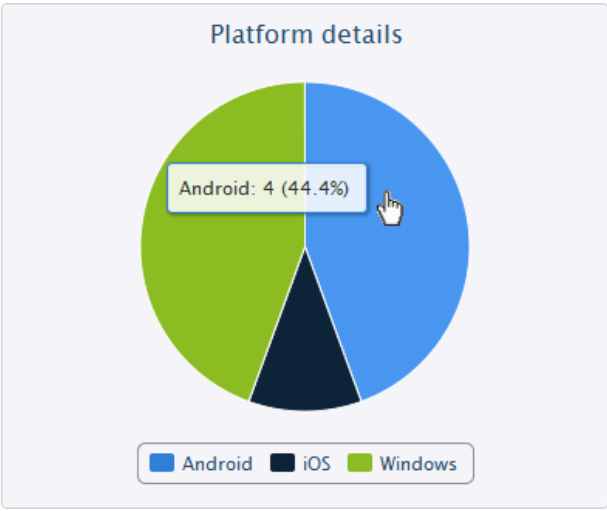
The Dashboard displays a snapshot summary of all the devices enrolled to Comodo Device Manager (CDM), their types, ownership and Antivirus (AV) scan status, as pie charts.

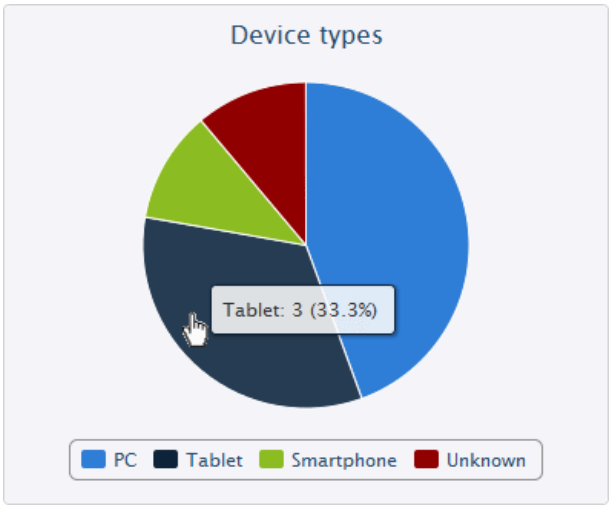
To open the 'Dashboard', click the Dashboard tab from the left hand side.



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.



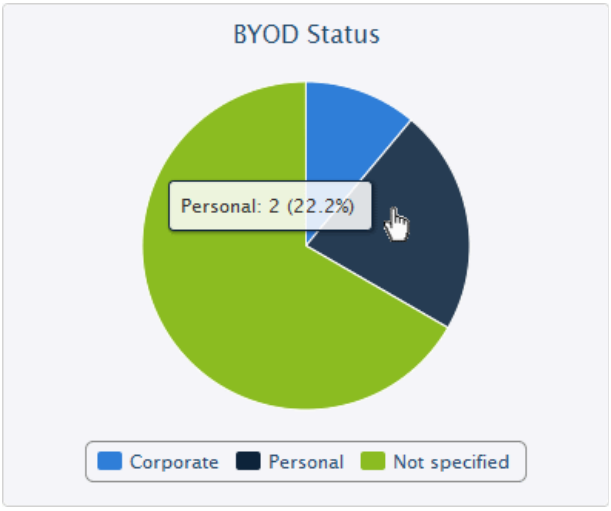


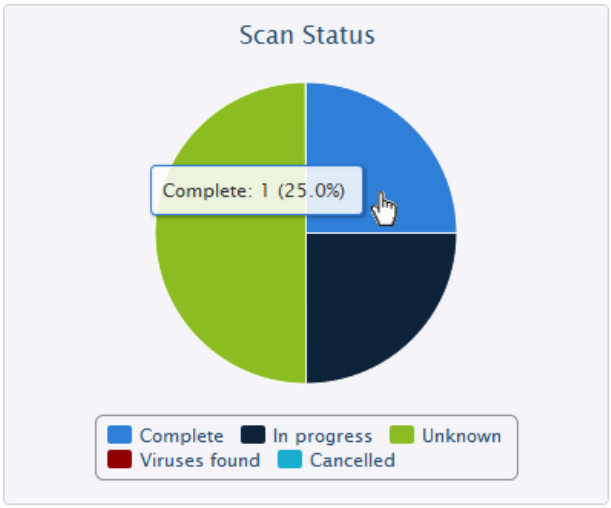
Device Types

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.

BYOD Status

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.





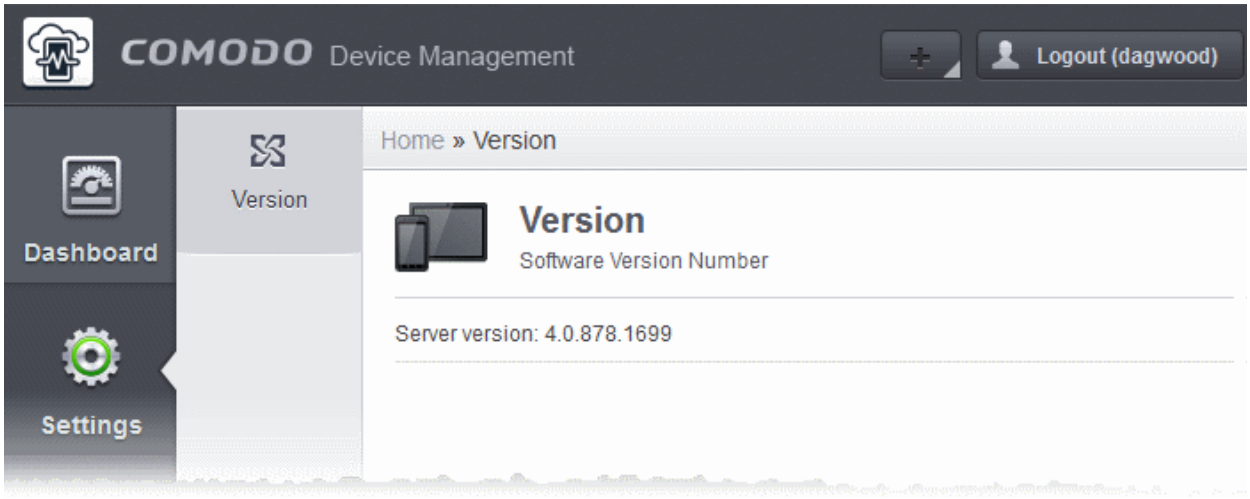
Scan Status

The 'Scan status' pie chart provides at-a-glance comparison of devices of different AV scan status, like completed, infected and so on. Hovering the mouse cursor or clicking over a sector displays a call-out providing details of the category.

5.2. Viewing Version Information

The Version information pane displays the version numbers of Comodo Device Manager's applications.

To open the 'Version' panel, click the 'Settings' tab from the left hand side.


COMODO Device Management
Logout (dagwood)
Dashboard
Settings
Version
Home » Version
Version
Software Version Number
Server version: 4.0.878.1699

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**

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