COMODO
Creating Trust Online®

Comodo
Mobile Device Manager

Software Version 1.0

Installation Guide

Guide Version 1.0.041114

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

Table of Contents

1.CMDM Setup

This document is intended to take administrators through the initial setup and configuration of Comodo Mobile Device Manager (CMDM). Before installing the application, administrators first need to obtain trusted SSL certificate(s) for two URLs – the front-end and back-end locations upon which they intend to host the solution. Comodo provide these fully trusted certificate(s) free of charge and administrators have the option of two separate certificates or a single wildcard depending on whether the two URLs are hosted on different domains or the same domain.

After signing up for Comodo Mobile Device Manager (CMDM), you will receive a confirmation mail containing a link to download the setup file. Please do not run this setup file yet, though, as there are a few vital steps you need to take before your environment is ready for the application to be installed.

1.1.System Requirements

Server Hardware

- Windows 64 bit system
- Processor – 2 GHz 64 bit processor
- Memory – 1 GB RAM minimum (recommended 2-16 GB)
- Hard Disk – 20 GB

Server Software

- Operating System

  The following operating systems are supported:

  - Windows Server 2008 R2
  - Windows Server 2012

Other Requirements

By default, the CMDM server requires:

- TCP Port 443 open for inbound connections to Administrative console.
- TCP Port 444 open tor inbound connections from devices.
- Valid DNS records for frontend and backend addresses.
- Valid SSL certificates for both frontend and backend domain names.
- Apple Push Certificate and key for Apple Push service. Refer to **Step 7 – Adding Apple Push Notification Certificate** for details.
- Google Cloud Messaging (GCM) token for Android push service. Refer to **Step 8 – Configuring Google Cloud Messaging (GCM) for Android** for details.

1.2. Step 1 – Frontend/backend URLs & DNS entries

The first task is to decide the URLs upon which you will host the frontend and backend parts of the application. Once you have decided, Comodo CA can provide you with free, fully trusted SSL certificate(s) if you do not already have them. Trusted certificates are required for the main application to function and to help with the application for an Apple Push Notification certificate.

Option 1 - Install on a existing domain(s) for which you already own an SSL certificate(s)

During setup you will be asked to configure the port numbers you wish CMDM to use on this domain and to upload your SSL certificates. You will not need to add new DNS entries. Example URL configuration: mycompany.com:443 for frontend; mycompany.com:444 for backend.

If you have a domain available and trusted SSL certificate(s), then you can skip to **Step 5 - installation of CMDM**

Option 2 – Install on new sub-domain(s) for which you already own a wildcard certificate

During setup you will be asked to configure the port numbers you wish CMDM to use on this domain and to upload your SSL certificates. You will also need to create a DNS entry for these new URL(s). Example URL configuration: sub1.mycompany.com:443 for frontend, sub2.mycompany.com:444 for backend.

If you have created new sub-domains, added DNS entries for them and have a trusted wildcard certificate to secure them, then you can skip to **Step 5 - installation of CMDM**

Option 3 – Install on entirely new domain(s) that you do not own trusted certificate(s) for

Then you need to obtain trusted SSL certificates for those URL(s) and set up DNS records for them. The type and quantity of certificate you require will depend on where you host.

i. Both front and backend on the same domain (or sub-domain) = one 'single domain' certificate
(example - yourdomain.com or sub.yourdomain.com for both frontend and backend)

ii. Front-end and backend on different domains = two 'single domain' certificates
(example - yourfirstdomain.com for frontend, yourseconddomain.com for backend)

iii. Front-end and backend on different sub-domains of the same domain = one wildcard certificate
(example - front.yourdomain.com for frontend, back.yourdomain.com for backend)

If you need certificates for your URLs, please move onto **Step 2 – Apply for SSL Certificates**

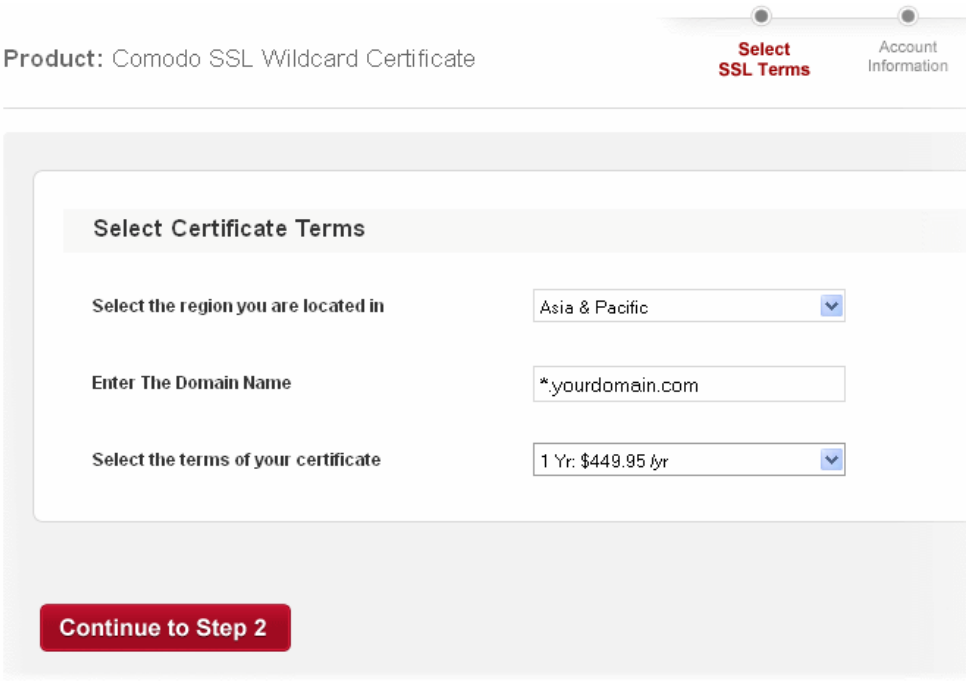
1.3. Step 2 – Apply for SSL Certificates

The trusted SSL certificates required for installation are provided free for CMDM customers. In short, you will complete the first 3 pages of the certificate application form and, when you get to the payment page, do not enter any card details, copy the order number, close your browser and contact Comodo support to free the order. Once the order is cleared, you will be sent a mail inviting you to log into your Comodo account where you can submit your Certificate Signing Request (CSR) and complete Domain Control Validation (DCV).

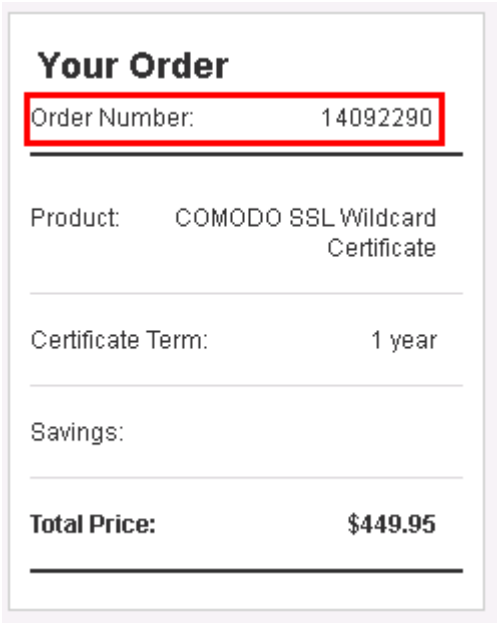
If your configuration is based around option 3(ii), then you will need to go through the order forms twice – one order for each single domain certificate.

To apply for your certificate(s)

- Visit **http://ssl.comodo.com/wildcard-ssl-certificates.php** or **http://ssl.comodo.com/comodo-ssl.php**
- Click the 'Buy Now' button.
- Enter your domain name. If you are getting a wildcard, make sure to add *. before the domain name. For example, *.yourdomain.com.
- Change the certificate term to one year.



- Click 'Continue to Step 2'
- On page 2, 'Account Information', select 'Returning Customer'.
- Enter the username and password you created on the CMDM application forms. Doing this will bind the certificate to your existing account and also means you will not have to complete 'Company Details' again.
- Fill out your contact details and leave 'Web Server Software' as 'Apache-ModSSL'. Leave the rest of the settings unchanged and click 'Continue'.
- Next, agree to the certificate Terms and Conditions, type your surname at the bottom and continue to the payment page. You must agree to the TOC or the order will not be created for you.
- On the payment page, copy and paste your order number and store it safely.



- Close the browser window.
- Send an email to **support@comodo.com** with subject line: 'CMDM SSL Provisioning – Order Number <*enter your order number*>.

- Our staff will clear the charge and you will receive a mail confirming your certificate order. This should be done very quickly after you send your request. However, please allow up to one working day for this action.
- Repeat the application form procedure to get a 2nd SSL certificate if required.
- Next:
    - If you need help to generate a Certificate Signing Request CSR, see **Step 3 – Generate your CSR** *(can be completed while you await the free certificate confirmation mail)*
    - Once you have generated a CSR you should proceed to **Step 4 – Complete Certificate Application** *(can only be completed once you have received the free certificate confirmation mail)*

1.4. Step 3 – Generate your CSR

A certificate signing request contains information about your domain and can be generated using a wide variety of utilities. If you are experienced with a popular web-server such as Apache, NGINX or IIS then please consult our CSR help documents -

https://support.comodo.com/index.php_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,128,96,1

Alternatively, you may use this simple tool to generate a CSR:

- Visit **http://ssltool.com/?action=csrGenerate**
- Enter yourdomain.com OR *.yourdomain.com in the 'CN' field.
- Leave 'Keysize' as '2048'
- Click 'Submit'
- Copy entire certificate request text and paste into a .txt file.
- Repeat the process if you need more than one certificate

Your CSR will look something like this:

-----BEGIN CERTIFICATE REQUEST-----

MIICXDCCAUQCAQAwFzEVMBMGA1UEAxQMKi5kb21haW4uY29tMIIBIjANBgkqhkiG

9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs91MERmFbB2lpzg5bLt99gsS5gTnoPoyxHUX

EOrgKWdBuS8DWTDa9oCbQwAKBRX5RjZO/3/9cQMht8orVyxmqCQ1HtoKEgBs1hTF

foy8Emy4TwH7xo4Dh/qIQv4gk5Xsv9dpTYYIWMQ8AuE=

-----END CERTIFICATE REQUEST-----

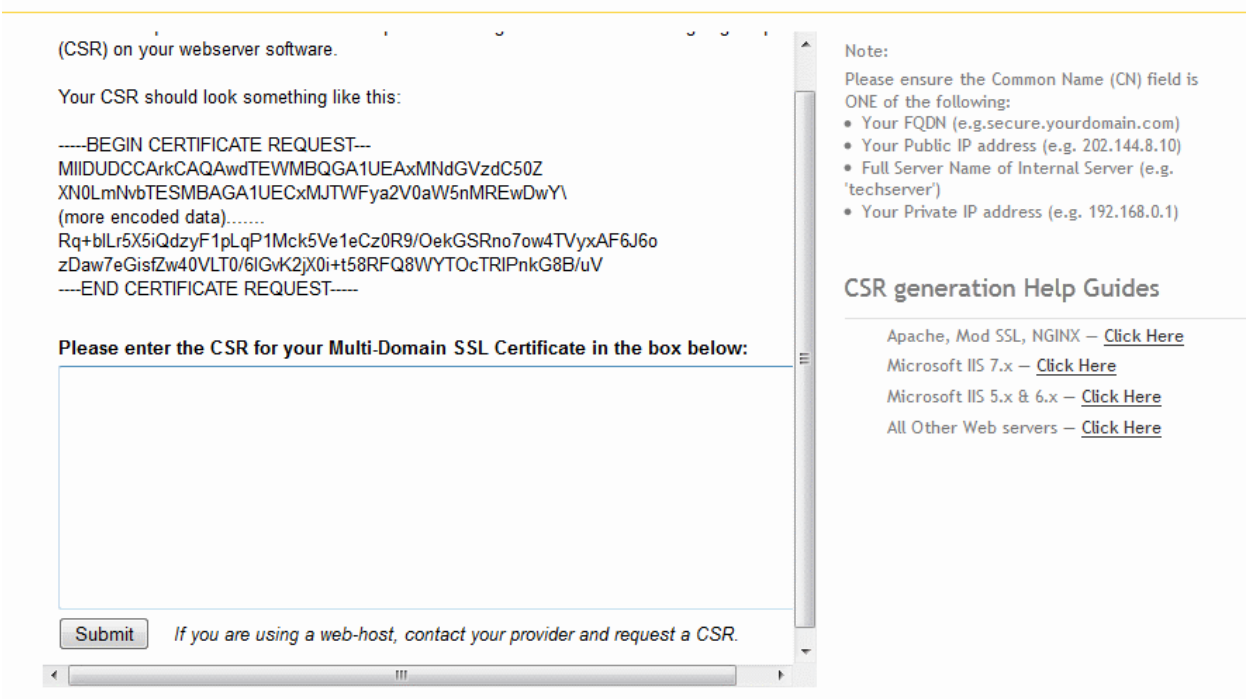
- Copy the entire certificate request text (including '---BEGIN...---' , '---END...---' text) and paste into a .txt file:
- Save this .txt file as you will need it shortly.

1.5. Step 4 – Complete Certificate Application

Once you have generated your CSR and have received your free certificate order confirmation mail, you should login to your Comodo account to complete the certificate application process.

- Please login at with your Comodo username and password.
    - New customers - you created your Comodo username and password on the Comodo Mobile Device Manager order form and should have re-entered it on the SSL application from in step 2. If you signed up for the certificate as a 'New Customer' (and thus created a different set of login credentials), then make sure you login at /frontpage using the SSL credentials.
- After logging in, you should see a box on this page called 'Incomplete Orders' which should list your certificate. Click the 'Accelerate' button.

- The 'Complete Your SSL Request' page contains a information that allows our SSL customers to finalize their orders. You need only concern yourself with two of these rows – 'Submit Your CSR' and 'Domain Control Validation'.
- Expand the 'Submit your CSR' row. Copy and paste your entire CSR into the space provided and click the 'Submit' button.



- Next, open the 'DCV' row and select an email address at the domain in your certificate application. You must be able to receive mails at this address to complete the DCV process.
- Your certificate(s) will be issued as soon as the CSR and DCV processes have been completed. If both have been done correctly, certificate issuance is usually immediate.
- You certificate will be emailed to you. Please save it to a secure location as you will need it during CMDM installation explained in Step 5. Alternatively, you can download your certificate as a zip file at any time if you log in at **http://secure.comodo.net/products/frontpage**, click 'SSL Certificate' then click 'Download as zip'.
- Contact **support@comodo.com** if your certificate has not arrived within an hour.
- When you have your certificate(s), please proceed onto step 5 – Install Comodo Mobile Device Manager.

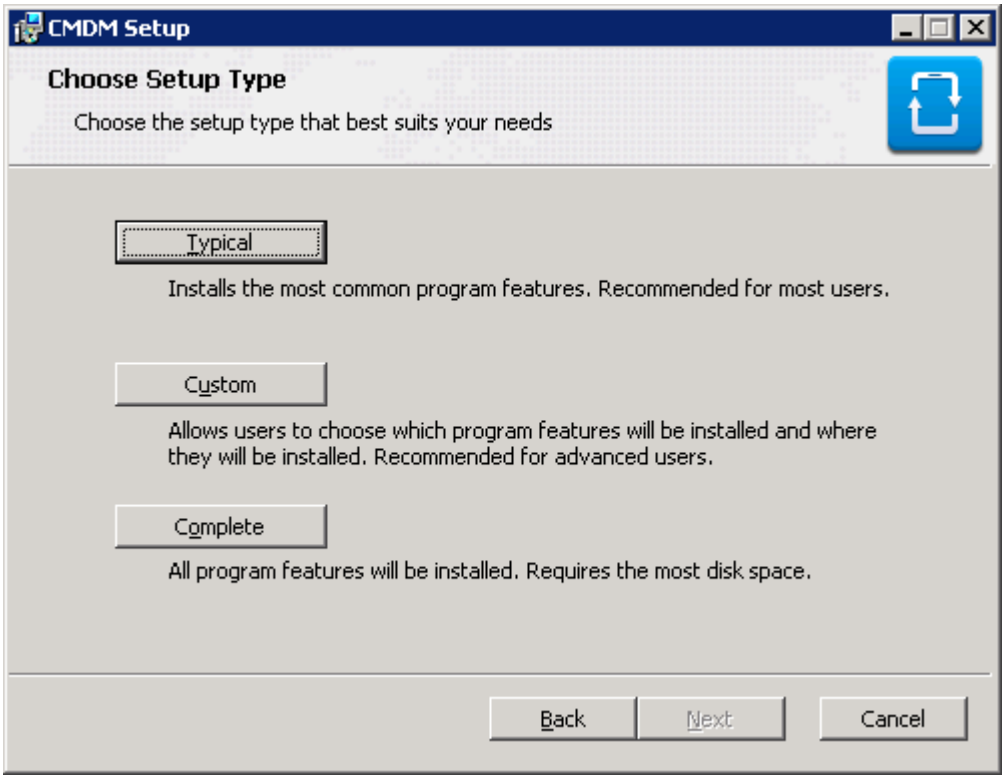
1.6. Step 5 – Install Comodo Mobile Device Manager

After collecting your certificate(s), open your Comodo Mobile Device Manager confirmation mail and download the setup file to your system.

To install CMDM

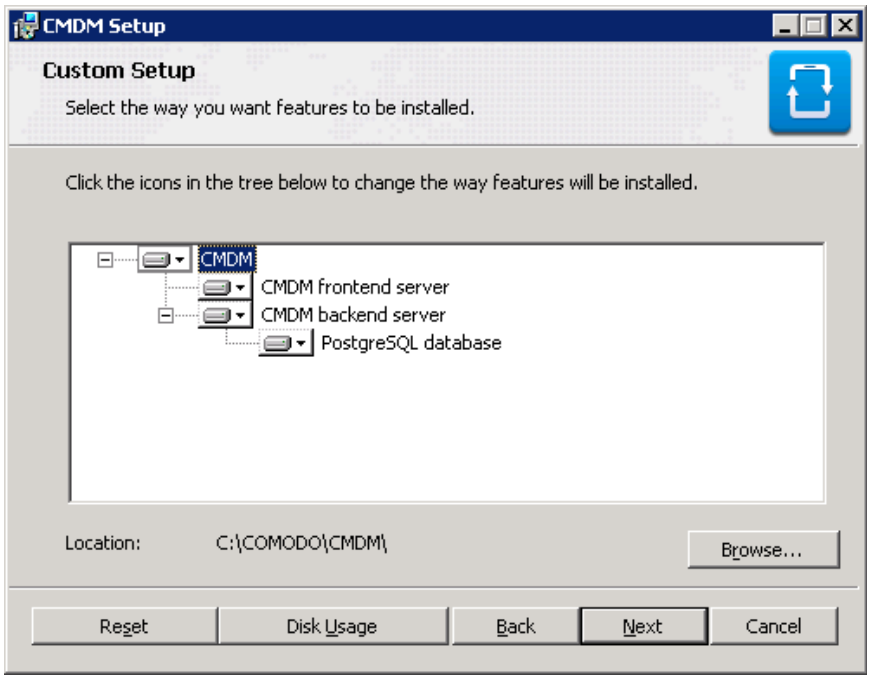
- Open the CMDM setup file and select 'Run':

- After agreeing to the end user license, you will be asked to choose which type of setup you would like to deploy:



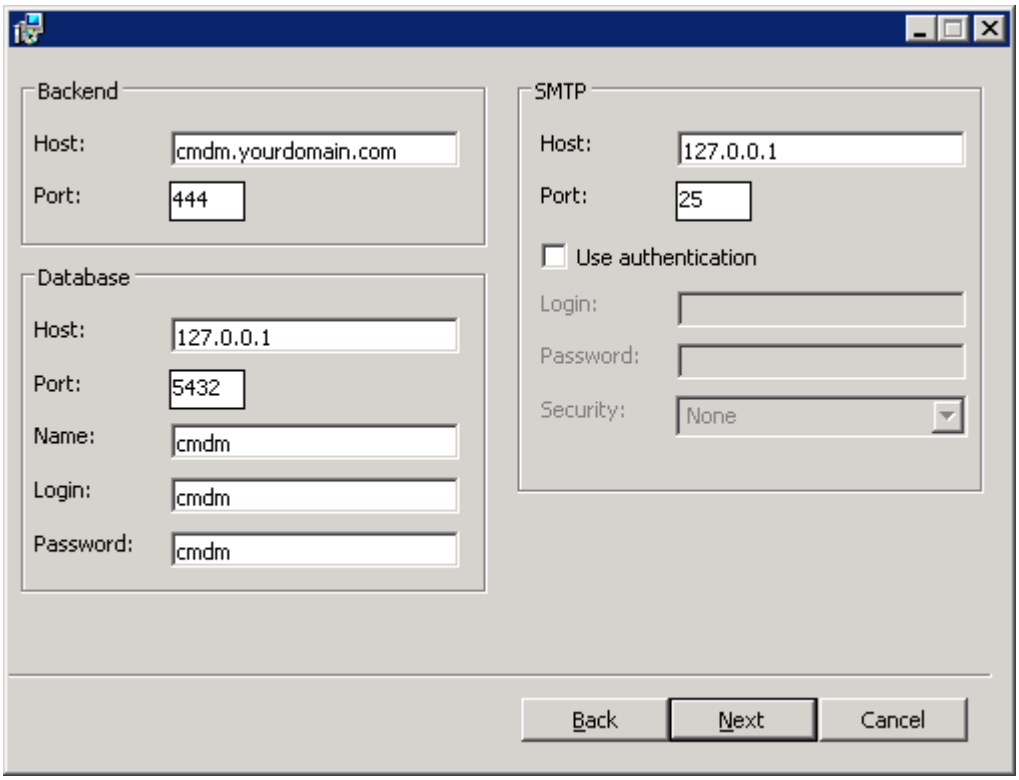
- **Typical** – Installs all components, CMDM frontend, backend and PostgreSQL to the default location C:\Comodo > CMDM
- **Custom** - Enables the administrator to choose which components are installed and to modify the installation path if required. The frontend could be installed on one server and the backend on another. If you choose to do this, then you need to run the CMDM setup file on both servers (and copy the appropriate certificate(s) over)
- **Complete** - Installs all components, CMDM frontend, backend and PostgreSQL to the default location C:\Comodo > CMDM

- The remainder of this section presumes you have selected the 'Custom' option.
- First, choose the components you wish to install and the installation directory:



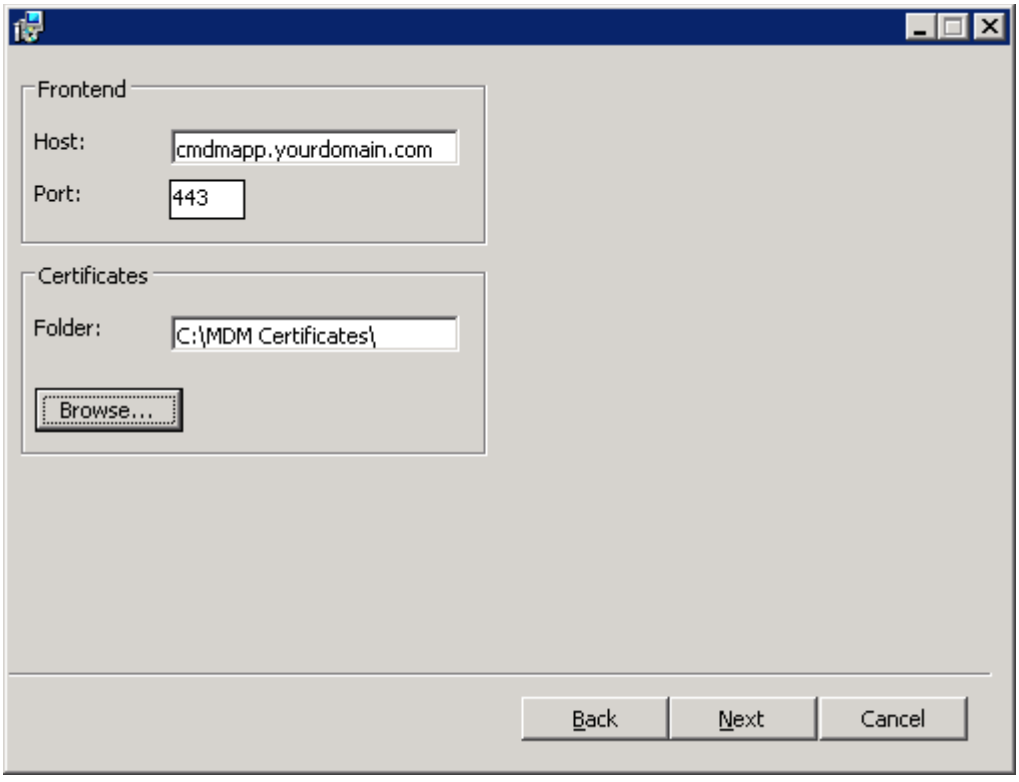
Custom Setup - Key	
Control	**Description**
	Current installation option. Click the ▼ icon to open a menu which allows you to select alternative installation options.
	Indicates that the component named to the right of the icon and all of its associated sub-components will be installed.
	Indicates that the component on the right will not be installed. Both frontend and backend components must be installed at some point. If you deselect one of them then you will need to run this installer later to install the missing items. If you already have a PostgreSQL database you wish to specify later, then you can deselect this item.
Browse....	Allows you to select a different installation folder (default = C:\COMODO\CMDM\)
Reset	Clears all user changes and reverts the dialog to default installation options.
Disk Usage	The combined disk space that will be taken up if the currently selected components are installed.
Back	Go back to the previous step in the installer
Next	The 'Next' button confirms your choices and continues onto the next stage of the installation process.
Cancel	The 'Cancel' button aborts the installation and quits the setup wizard.

- When you are happy with your setup selection, click 'Next' to proceed to backend configuration.



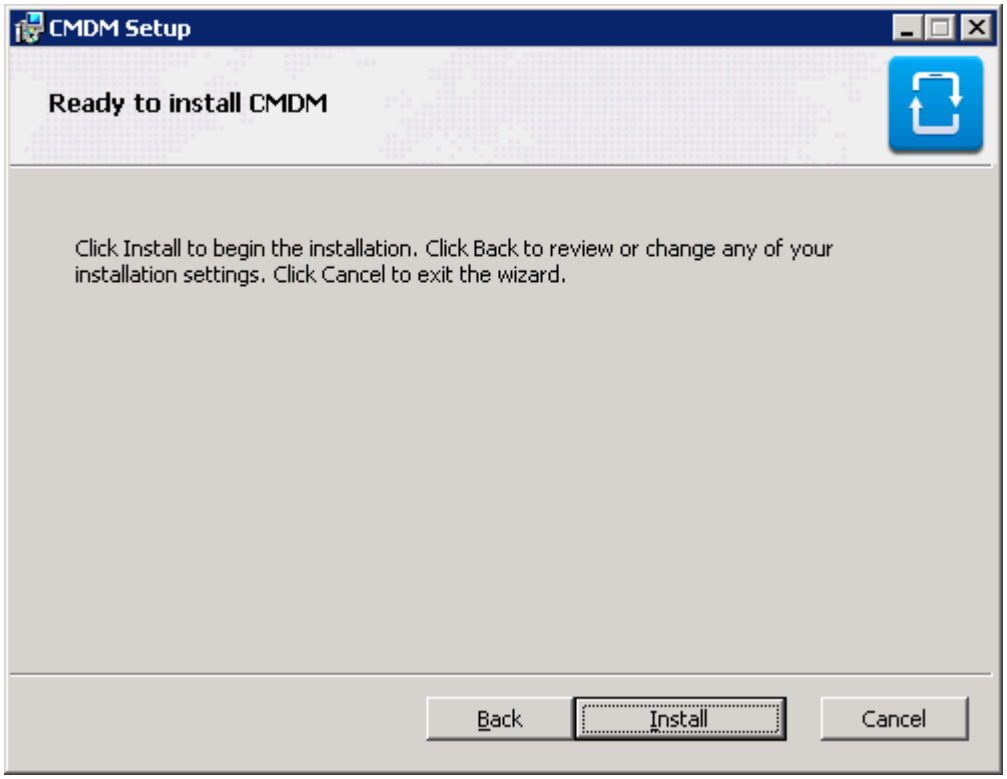
Backend, Database and SMTP – Table of Parameters		
Backend	Host	Enter the URL that will host the CMDM backend. This should match the URL in the certificate (or one of the certificates) you applied for in step 2.
	Port	Enter the port number through which the frontend will communicate with the backend.
Database	Host	Enter the IP address of the host where the database is installed. A PostgreSQL database is built into the CMDM setup file. If you are going with a default installation then you do not need to edit the host field (or, indeed, any of the 'database' fields). However, if you wish to point to an existing PostgreSQL 9.1 (or higher) database then modify these fields accordingly.
	Port	Enter the port number through which CMDM should connect to the database.
	Name	Enter the name of the database.
	Login	Enter the username and password for the database
	Password	
SMTP	Host	Enter the host address of SMTP server (required for sending system mails to enrolled end-users)
	Port	Enter the outgoing mail port number
	Use authentication	If checked, enter the login and password for the email account. Select security type from the drop-down.

Click 'Next' to confirm your choices. Frontend configuration and SSL certificate upload is next:

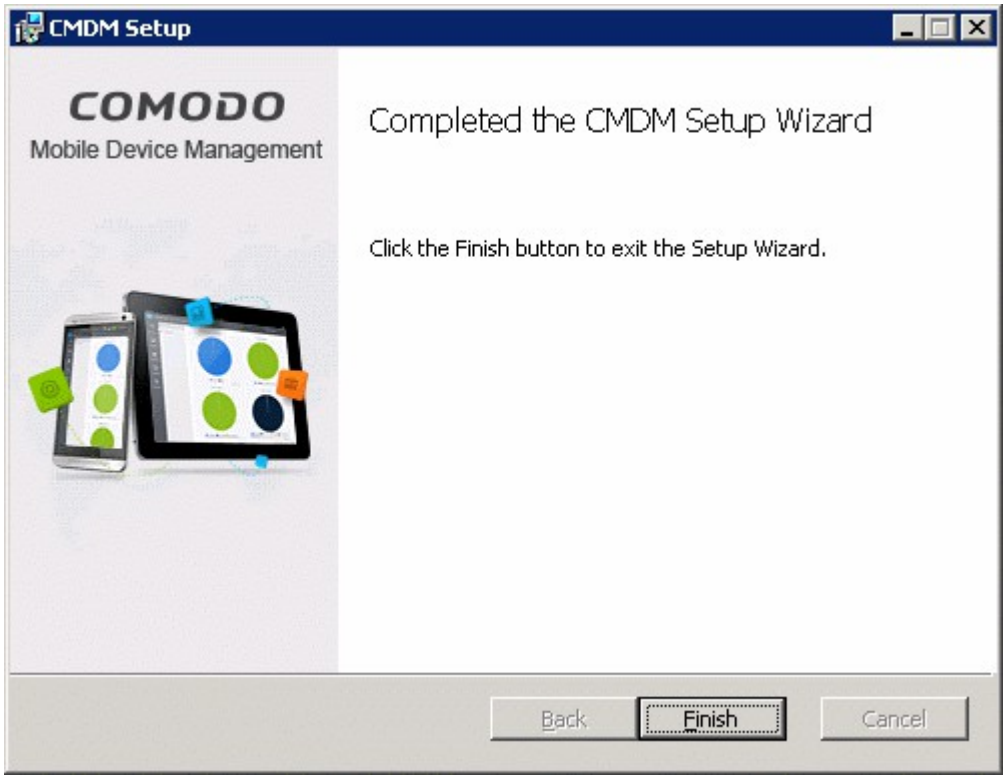


- Host - The URL that will host the CMDM frontend. This should match the URL in the certificate (or one of the certificates) you applied for in step 2.
- Enter the port number in the Port field. Default = 443.
- Certificates folder – Specify the location to which you saved the frontend certificate from step 2.
- Click 'Next' when you are satisfied with your choices.

- 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:



- Your next step is to activate your CMDM license. To open the application, please open an internet browser (Chrome or Comodo Dragon preferred) and enter your 'frontend' URL in the address bar.

1.7. Step 6 – Activating Your License

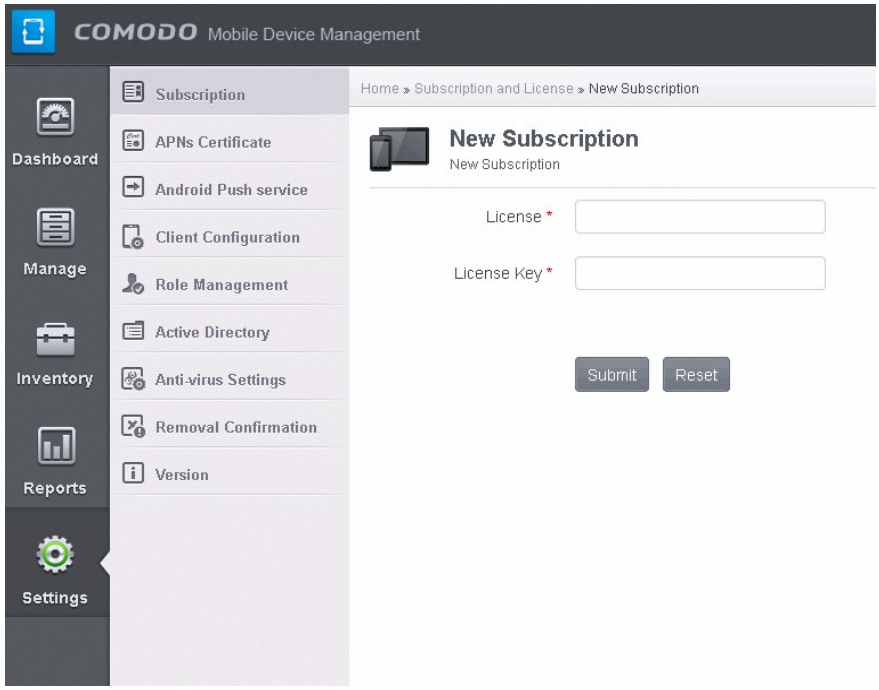
You need to activate your license before you can start to enroll users and devices.

To activate:

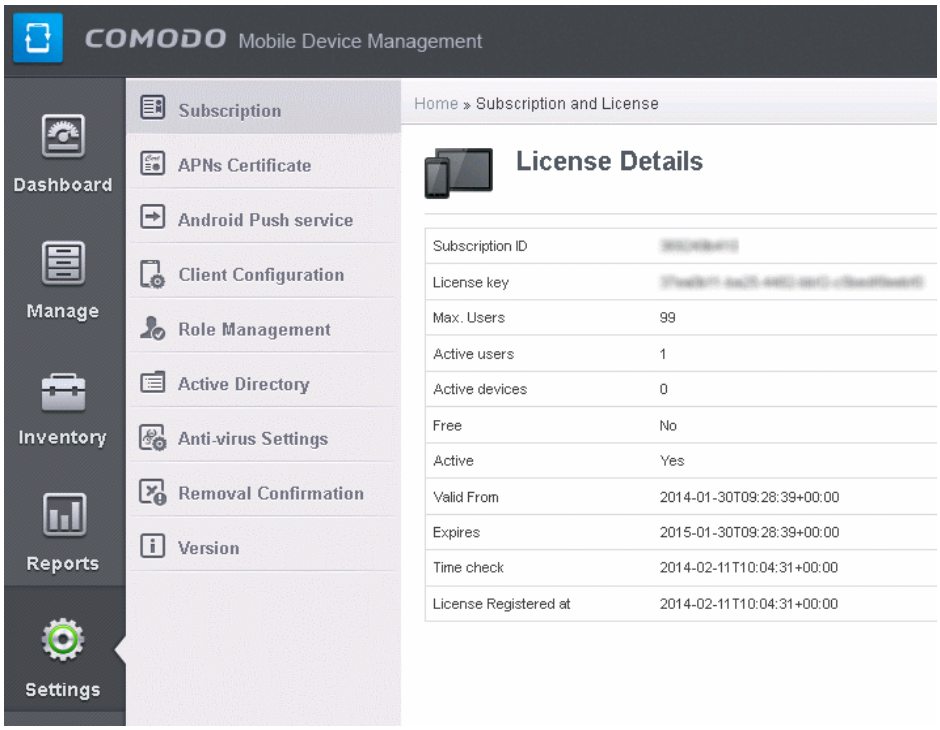
- Open an internet browser (Chrome or Comodo Dragon preferred) and enter your 'frontend' URL into the address bar. This will open the initial login screen:

- Login using the following credentials: Username: admin Password : admin
- You can (and should) change these to a unique username and strong password at any time *after* license activation. 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.

After logging in you need to enter your subscription ID and license key at the 'New Subscription' screen. Both these items can be found in your CMDM confirmation email.



After your license has been validated you will be able to start using the application. On subsequent visits you will only need to enter your username and password.

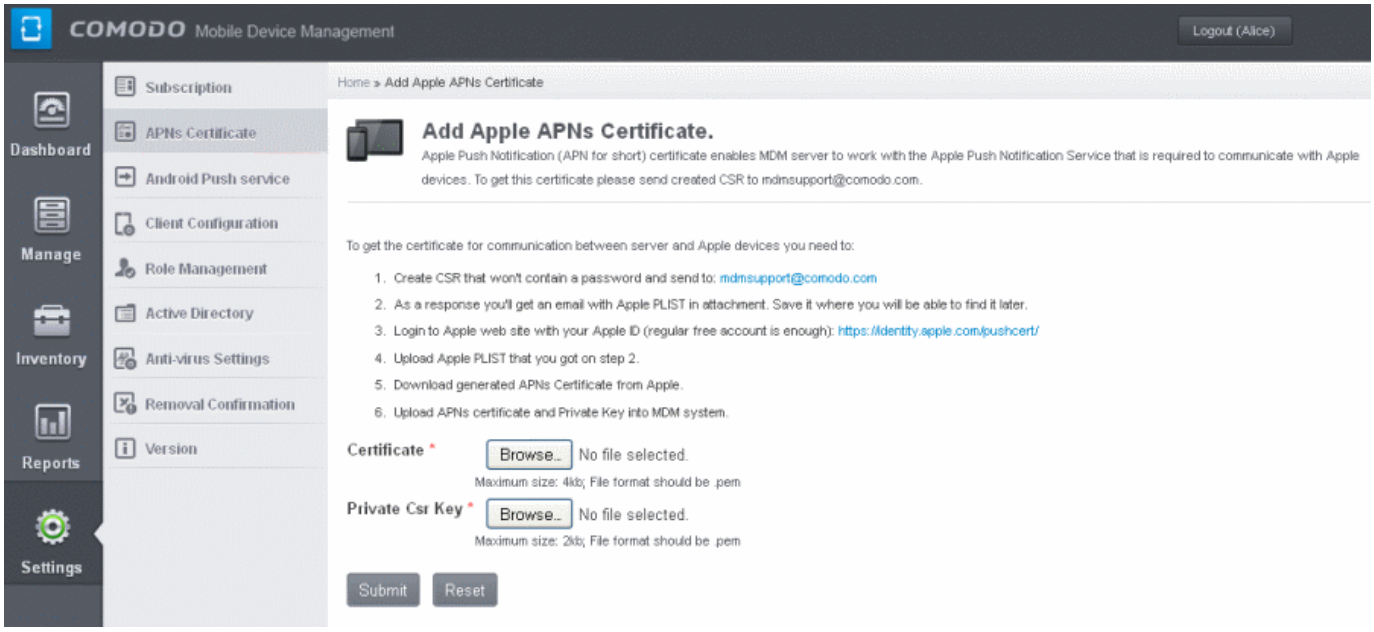


For your first task now that setup is complete, we advise you configure Apple Push Notification

1.8. Step 7 – Add an Apple Push Notification (APNs) 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** – Create a CSR (without password) and send it to **mdmsupport@comodo.com**. Store the Private Key safely. See **Step 3 – Generate your CSR** for help with this.
- **Step 2** – Comodo will sign your CSR with their Apple MDM certificate and send you an Apple PLIST as an attachment
- **Step 3** – 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**.
- **Step 4** – At **https://identity.apple.com/pushcert/**, upload the Apple PLIST that was sent to you in step 2
- **Step 5** – Download the APN certificate and save it to your local drive.
- **Step 6** – Finally upload the APN certificate and private key to CMDM. To do so, go to 'Settings' and click 'APNs Certificate'



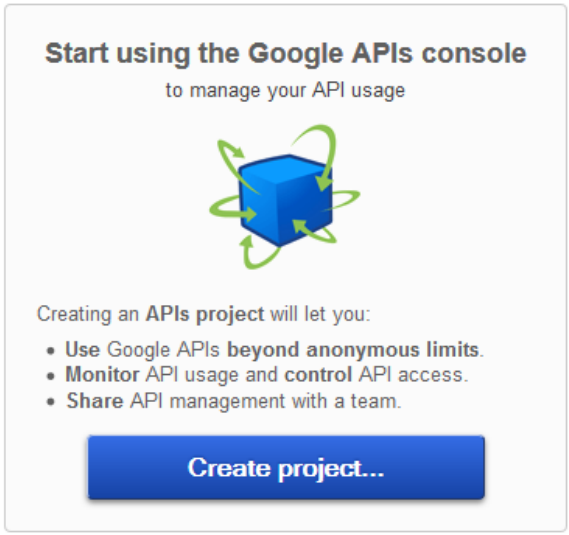
CMDM will be able to communicate with iOS devices once the certificate and private key have been uploaded.

1.9. Step 8 – Configuring Google Cloud Messaging (GCM) for Android

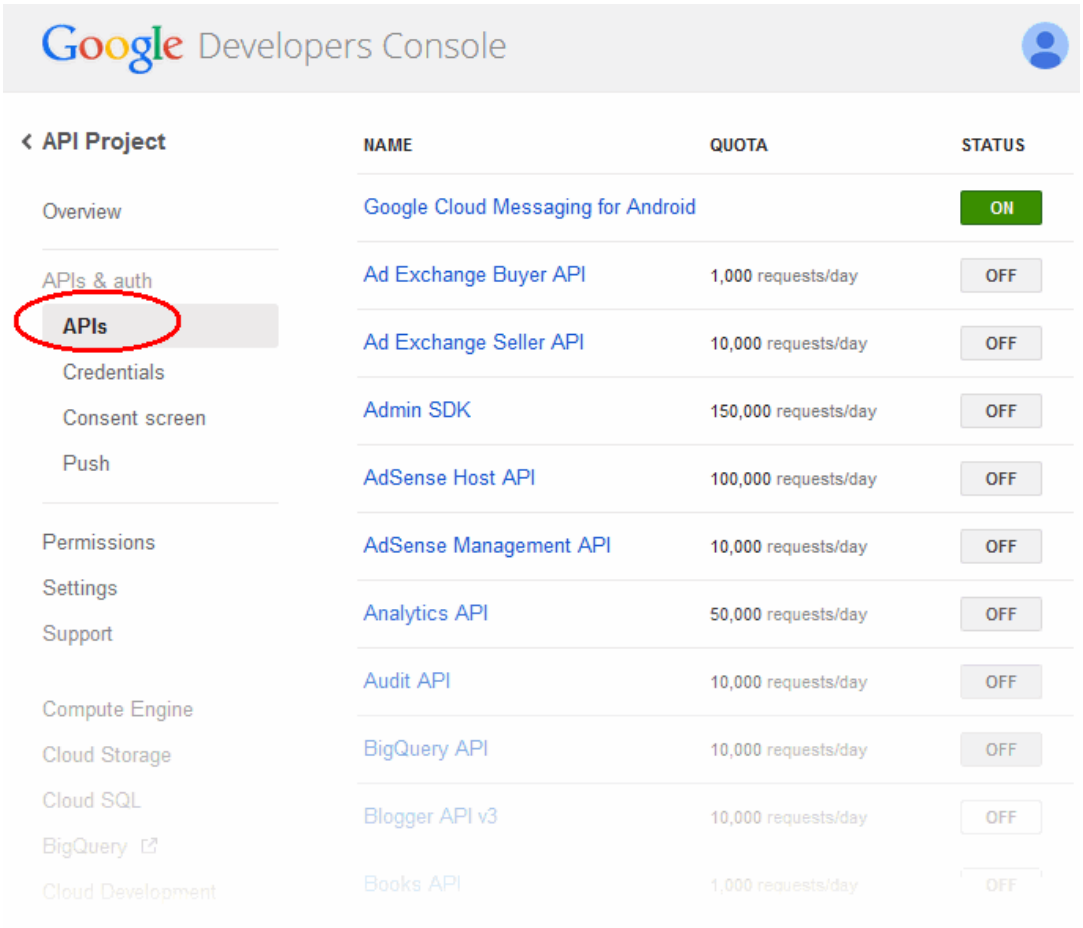
In order to communicate with Android devices you need to install a Google Cloud Messaging token on each device. This token is seamlessly installed during the enrollment of each device.

CMDM ships with a default API token which is used to communicate with enrolled Android devices. This default token is hardcoded and is not visible in the interface. You can, however, generate and upload a unique Android GCM token

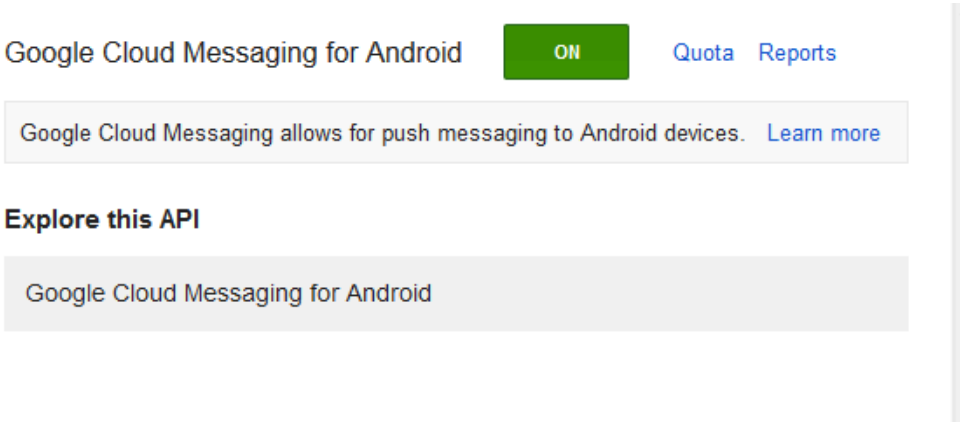
To generate a token, you must have created a Mobile Backend Project at **http://code.google.com/apis/console**.



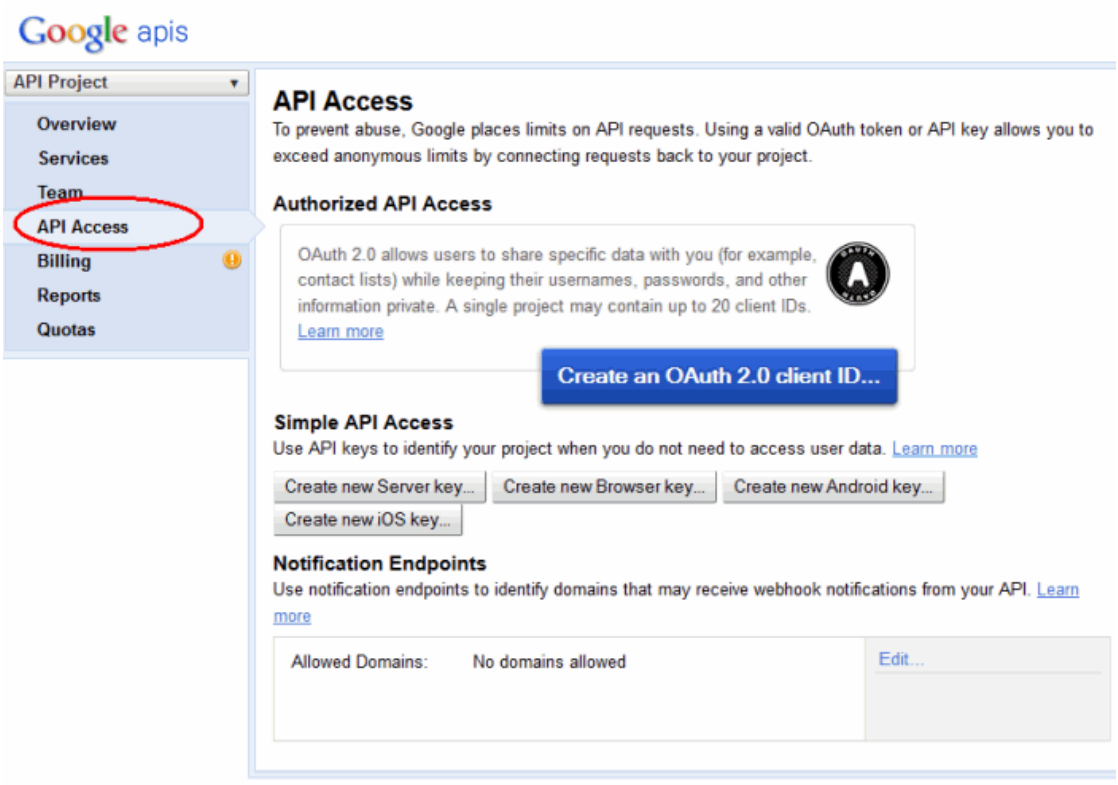
- **Step 1** – Open the Google API Console at **http://code.google.com/apis/console** and select 'Mobile Backend Project' from the pull down menu at top left side.
- **Step 2** – Click 'Services'.



- **Step 3** – Scroll down the page and in the list of available services, locate 'Google Cloud Messaging for Android' and click the toggle button to 'ON'.

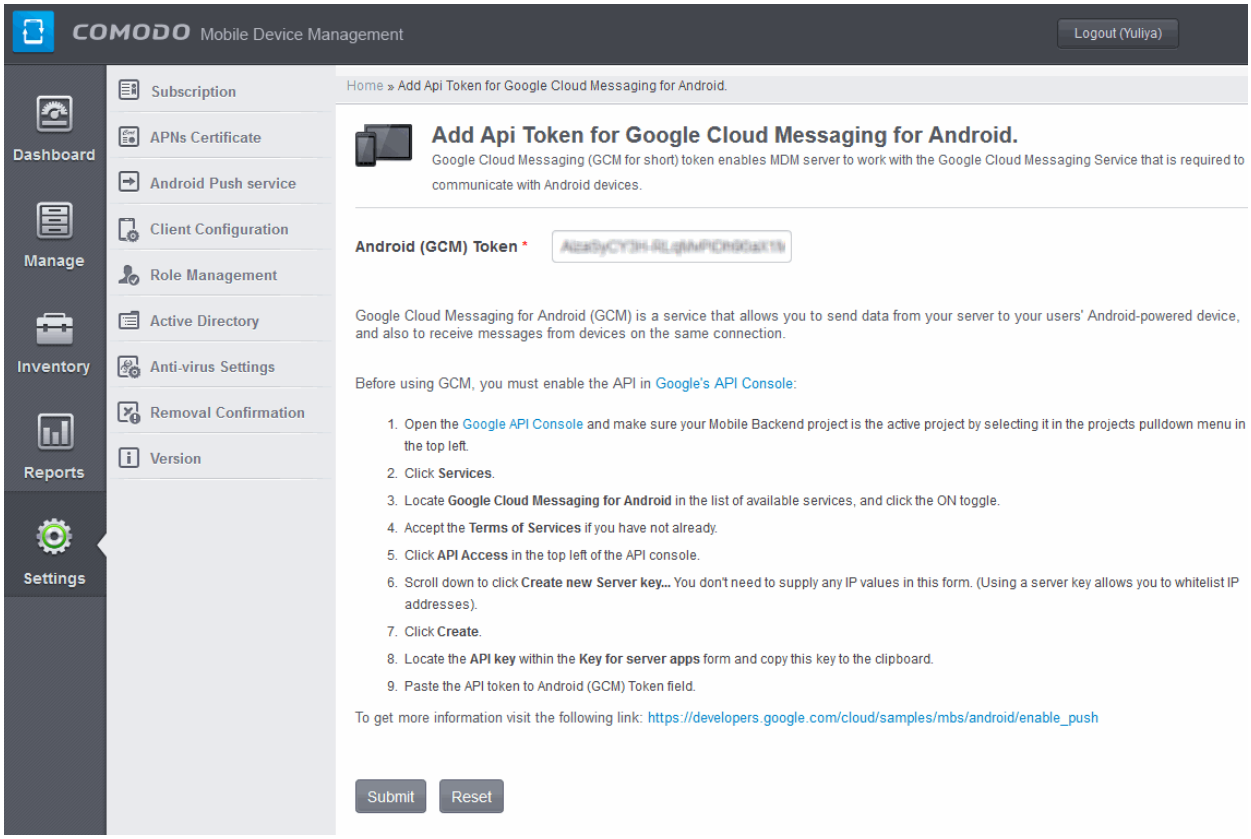


- **Step 4** – Accept the 'Terms of Services', if you have not done so already.



- **Step 5** – Click 'Google cloud Messaging for Android > Reports'. Click the 'API Access' in the top left of the 'API Project' console.
- **Step 6** – Scroll down and click 'Create new Server key'. No need to supply any IP values in this form.

- **Step 7** – Click 'Create'.
- **Step 8** – Locate the API key within the 'Key for server apps' form and copy this key to the clipboard.
- **Step 9** – Copy the API key from the clipboard and paste it in the text box beside Android (GCM) Token in the 'Settings' > 'Android push Service' page.



- **Step 10** - Click the 'Submit' button to finalize configuration.

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**.