

Comodo Device Manager

Software Version 4.0

Installation Guide

Guide Version 4.0.061815

Table of Contents

1.Comodo Device Manager Setup	3
1.1.System Requirements.....	3
Step 1 - Frontend/backend URLs & DNS entries.....	4
Step 2 - Apply for SSL Certificates.....	4
Step 3 - Generate your CSR.....	6
Step 4 - Complete Certificate Application	8
Step 5 - Install Comodo Device Manager.....	9
Step 6 - Activating Your License.....	15
Step 7 - Configuring SMTP Settings.....	18
Step 8 - Add an Apple Push Notification (APNs) Certificate	20
Step 9 - Configuring Google Cloud Messaging (GCM) for Android.....	26
Step 10 - Upload your Enterprise/Custom Android App (Optional).....	31
2.Reconfiguring CDM	32
About Comodo.....	36

1. Comodo Device Manager Setup

This document is intended to take administrators through the initial setup and configuration of Comodo Device Manager (CDM).

Before installing the application, administrators first need to install SSL certificate(s) on two URLs - the front-end and back-end locations upon which they intend to host the solution.

At this point you have two options:

- Use browser trusted certificates. Comodo provide these fully trusted certificate(s) free of charge. If you choose this option, you need to complete all steps in this guide.
- Use self signed certificates. Best for fast set up but end-users will be asked to trust the certificate upon connection. See box below for more details.

Fastest Setup - Use self-signed Certificates

- Skip to **Step 5** of this guide
- During installation, enter your server IP as the 'Backend' and 'Frontend' host entries
- Select the 'Use Self-Signed certificates' option
- Complete steps 6, 7 and 8

Please note that end-users will see an error message upon connection and will be asked to trust the certificate.

As an alternative to this guide, a video explaining the CDM setup process is available [here](#).

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 CDM server requires:

- TCP Port 443 open for inbound connections to Administrative console.
- TCP Port 444 open for 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.

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 CDM to function correctly and to help with the application for an Apple Push Notification certificate.

Tip: If you are evaluating the application and wish to avoid the SSL certificate application process, then you can use self-signed certificates on your server instead. Self-signed certificates are not publicly trusted so your users will have to agree to trust the certificate when they connect from their device. To install CDM with self-signed certificates, skip the next three steps and proceed to Step 5 to begin the installation process.

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 CDM 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 CDM**

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 CDM 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 CDM**

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**

Step 2 - Apply for SSL Certificates

The trusted SSL certificates required for installation are provided free for CDM 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.

Product: Comodo SSL Wildcard Certificate

Select SSL Terms Account Information

Select Certificate Terms

Select the region you are located in Asia & Pacific

Enter The Domain Name *.yourdomain.com

Select the terms of your certificate 1 Yr: \$449.95/yr

Continue to Step 2

- Click 'Continue to Step 2'
- On page 2, 'Account Information', select 'Returning Customer'.
- Enter the username and password you created on the CDM 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.

Your Order

Order Number:	14092290
Product:	COMODO SSL Wildcard Certificate
Certificate Term:	1 year
Savings:	
Total Price:	\$449.95

- Close the browser window.
- Send an email to mdmsupport@comodo.com with subject line: 'CDM 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)

Step 3 - Generate your CSR


CDM has a built in tool which allows you to generate a Certificate Signing Request (CSR) for your CDM certificate. A certificate signing request contains information about your company and the domain upon which you are hosting CDM.

To generate a CSR:

- Visit <https://mdmsupport.comodo.com/csr/generate>
- Login using your Comodo Account Management credentials. This is the username and password you originally created on the CDM application forms and which you should have used while applying for your certificate in **the previous step**.
 - Note: If you signed up for the certificate as a 'New Customer' in step 2 (and thus created a different set of login credentials), then make sure you login at /comodo-members.php using the SSL username and password.

COMODO Web Application

Login

 **Login**
Please fill out the following form with your login credentials:

* Username

* Password

* Verification Code

iocedb
[Get a new code](#)

Please enter the letters as they are shown in the image above.
Letters are not case-sensitive.
Fields with * are required.


Login

Remember me next time

- Choose the 'Generate CSR' tab and fill out and submit the form to generate your CSR.

COMODO Web Application

Generate CSR Application Wrapper Logout (triumph)

 **Generate CSR**
You can generate CSR here.

Fields with * are required.

* Country Name [C]

* Common Name [CN]
e.g. server Fully Qualified Domain Name

* Organization Name [O]

Email Address

State or Province Name [ST]

Organizational Unit [OU]
e.g. section

Locality Name [L]
e.g. city

Generate and Download

- Enter the domain name where your CDM portal is to be hosted in the 'Common Name' field (for example mdm.yourcompanyname.com or *.yourdomain.com)
- 'Organization Name' must match the company name in your CDM license. 'Organizational Unit' can be a department in your company.
- Click 'Generate and Download' to obtain your CSR.
- Save the .zip file containing your CSR and private key to your local drive. You will need it in the next step.

Next - **Step 4 - Complete Certificate Application**

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 <https://www.comodo.com/login/comodo-members.php> with your Comodo username and password. Use the 'Comodo Certificate Authority' login box. You originally 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.
 - Note: If you signed up for the certificate as a 'New Customer' in step 2 (and thus created a different set of login credentials), then make sure you login at /comodo-members.php using the username and password

you entered on the SSL application form.

- After logging in, you should see a box on this page called 'Incomplete Orders' which should list your certificate. Click the 'Accelerate' button.

Order # (date) SSL Product Type	Status
STATUS (2014-04-13) PremiumSSL Certificate for 88	Awaiting Payment Accelerate

- 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.

(CSR) on your webserver software.

Your CSR should look something like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwTEWMBQGA1UEAxMNdGVzdC50Z
XN0LmNvbTESMBAGA1UECXMJTWFya2V0aW5nMREwDwYI
(more encoded data).....
Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6o
zDaw7eGisfZw40VLT0/6IGvK2jX0i+58RFQ8WYTOcTRIPnkG8B/uV
-----END CERTIFICATE REQUEST-----
```

Please enter the CSR for your Multi-Domain SSL Certificate in the box below:

If you are using a web-host, contact your provider and request a CSR.

Note:

Please ensure the Common Name (CN) field is ONE of the following:

- Your FQDN (e.g.secure.yourdomain.com)
- Your Public IP address (e.g. 202.144.8.10)
- Full Server Name of Internal Server (e.g. 'techserver')
- Your Private IP address (e.g. 192.168.0.1)

CSR generation Help Guides

- Apache, Mod SSL, NGINX – [Click Here](#)
- Microsoft IIS 7.x – [Click Here](#)
- Microsoft IIS 5.x & 6.x – [Click Here](#)
- All Other Web servers – [Click Here](#)

- 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 CDM 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 mdmsupport@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.

Step 5 - Install Comodo Device Manager

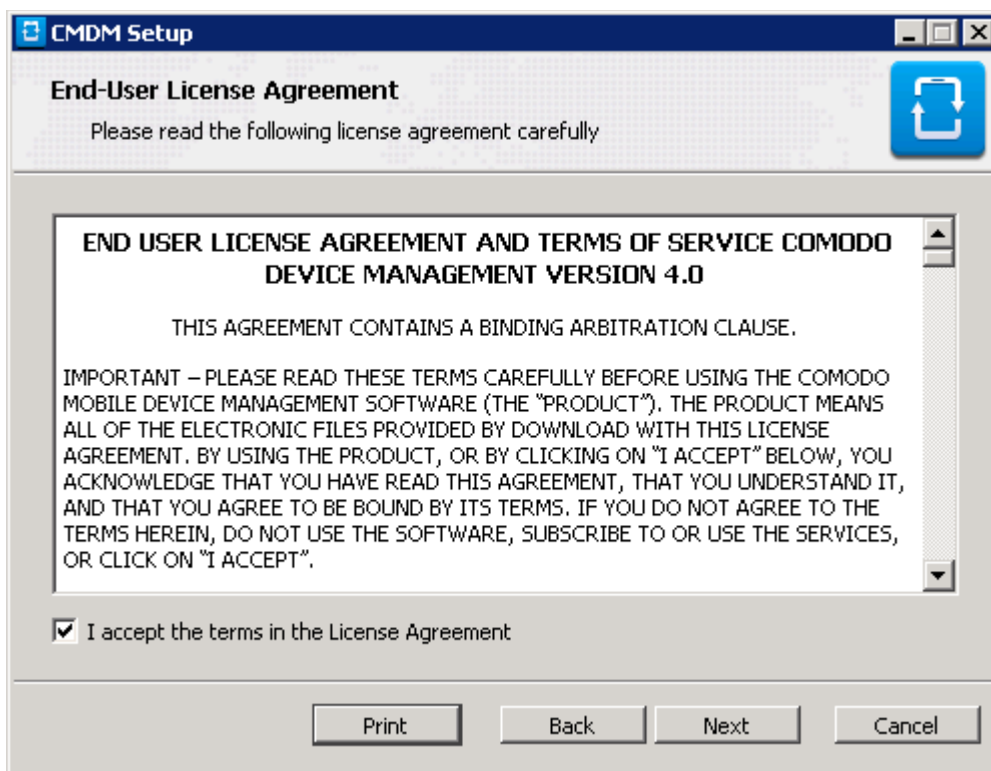
After collecting your certificate(s), open your Comodo Device Manager confirmation mail and download the setup file to your system.

To install CDM

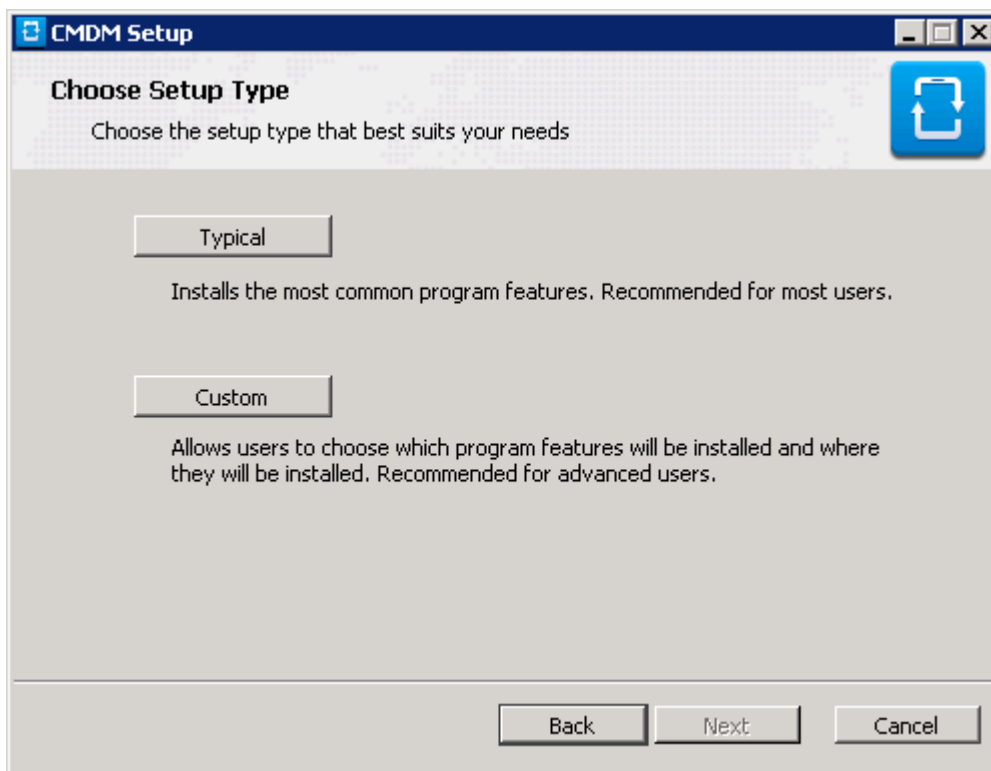
- Double click on the CDM setup file or right click on the file and choose 'Open'



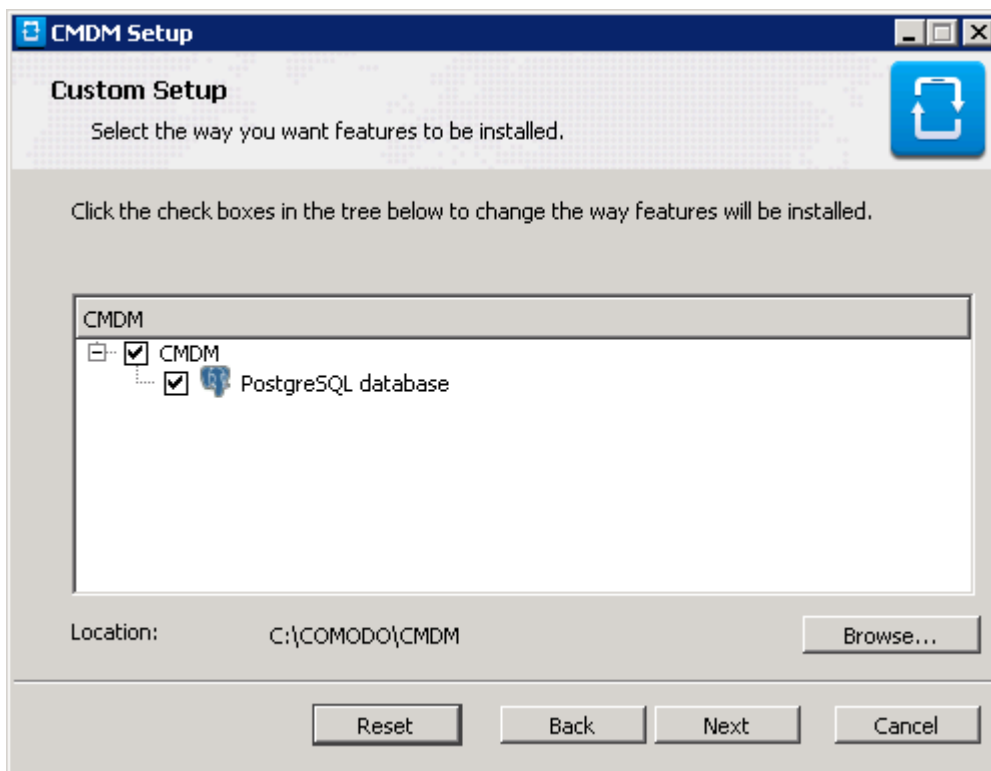
- Click 'Next'.





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

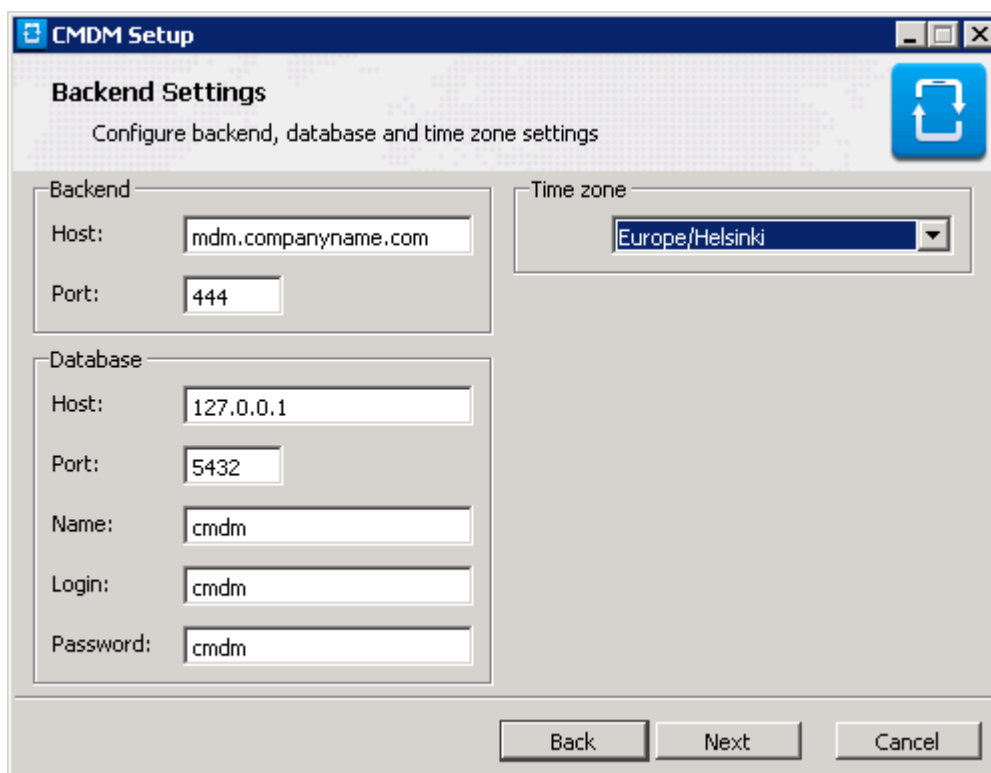


- **Typical** - Installs all components, CDM frontend, backend and PostgreSQL to the default location C:\Comodo > CDM
- **Custom** - Enables you to choose which components are installed and to modify the installation path if required. You can choose to install the CDM frontend and backend servers and the PostgreSQL database at different servers.



Custom Setup - Key	
Control	Description
<input checked="" type="checkbox"/>	Current installation option.
<input checked="" type="checkbox"/> 	Indicates that the component named to the right of the icon and all of its associated sub-components will be installed. Click  to open a menu which allows you to select /deselect components.
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.
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.

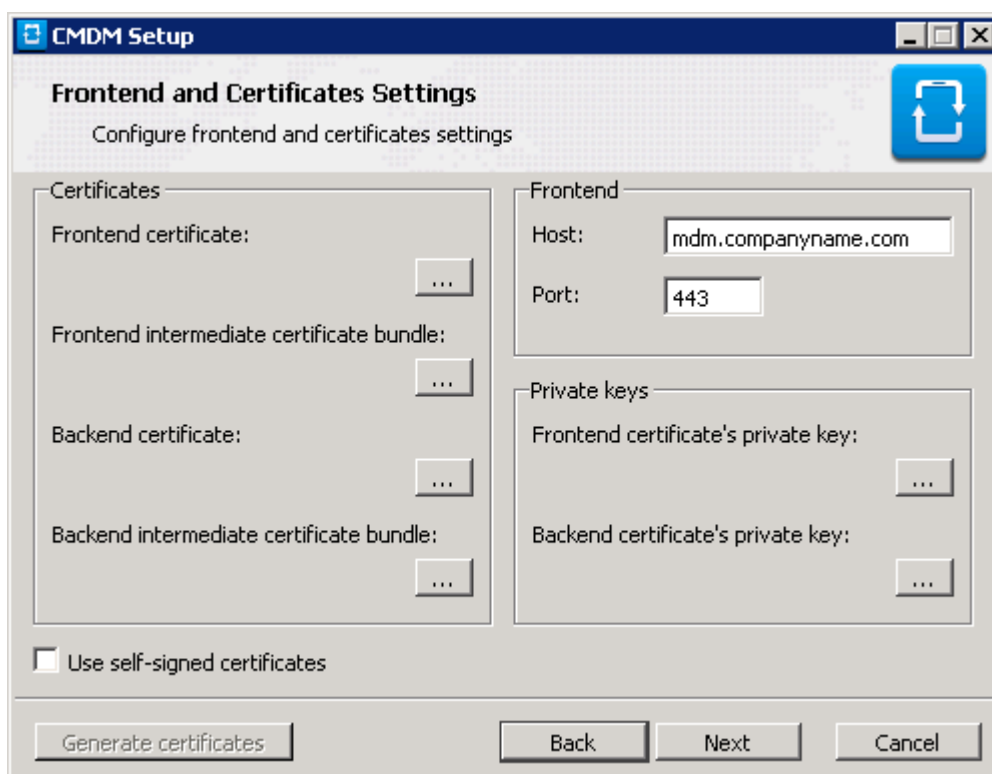
- The remainder of this section presumes you have selected the 'Typical' option.
- First, click 'Next' to proceed to backend configuration.



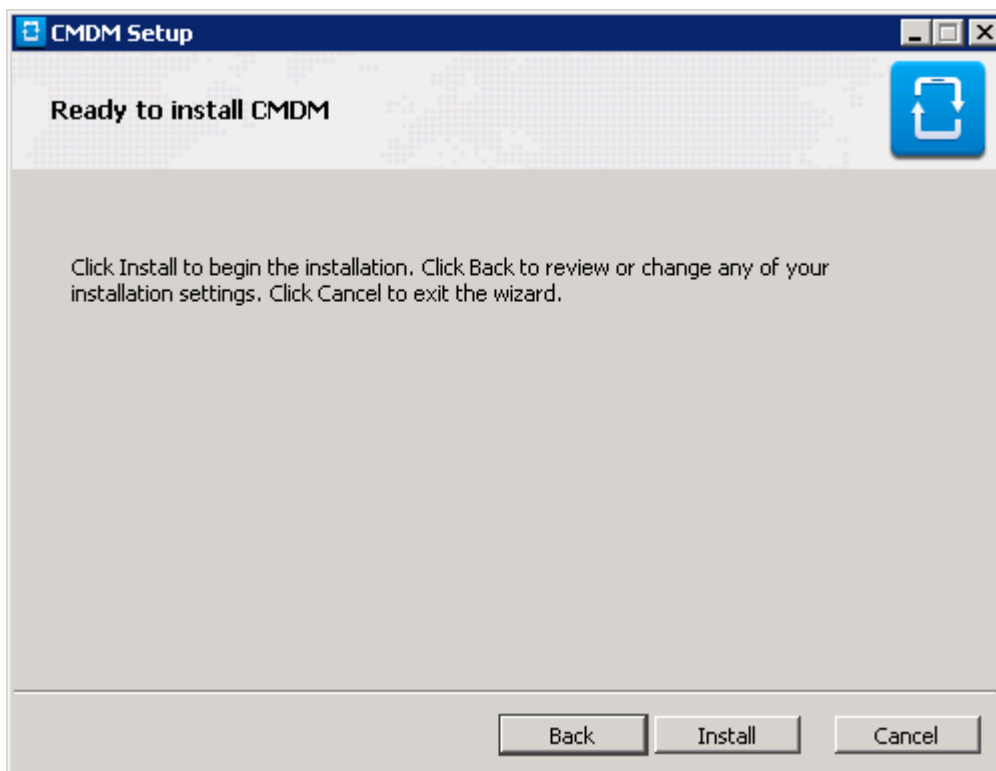
Backend, Database and Time Zone - Table of Parameters		
Parameter		Description
Backend	Host	Enter the URL that will host the CDM backend. This should match the URL in the certificate (or one of the certificates) you applied for in step 2 . If you are going to use self-signed certificate, then enter the public IP of the server.
	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 CDM 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 CDM should connect to the database.
	Name	Enter the name of the database.
	Login	
	Password	Enter the username and password for the database
Time Zone	Select your time zone from the drop-down	

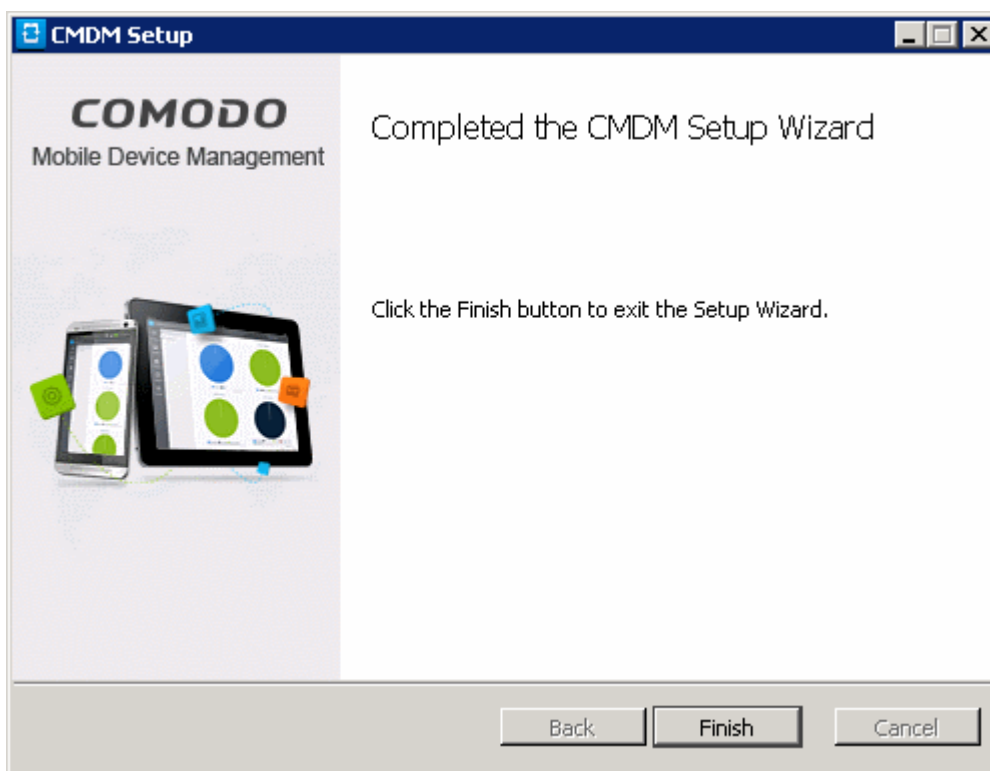
- Click 'Next' to confirm your choices. Frontend configuration and SSL certificate upload is next:



- Host - The URL that will host the CDM frontend. This should match the URL in the certificate (or one of the certificates) you applied for in step 2. If you are going to use self-signed certificate, then enter the public IP of the server.
- Enter the port number in the Port field. Default = 443.
- Certificates - Specify the location to which you saved the frontend and backend certificates and the frontend and backend intermediate certificates.
- Private keys - Specify the location to which you saved the frontend and backend certificates' private keys
- Use self-signed certificates - Select this option if you have not obtained trusted SSL certificates and want to use the application for trial purpose. Click the 'Generate certificates' button after selecting the 'Use self-signed certificates' checkbox.
- Click 'Next' when you are satisfied with your choices.
- The Installation will commence after you click the 'Install' button in the next dialog. 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:



Note: If required, you can reconfigure your CDM installation at a later time using the 'Reconfiguration Wizard'. The wizard can be opened on the CDM server machine by clicking 'Start > Programs > COMODO > CMDM > CMDM Configuration Wizard'. For more details, see the section '**Reconfiguring CDM**' section.

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

Step 6 - Activating Your License

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

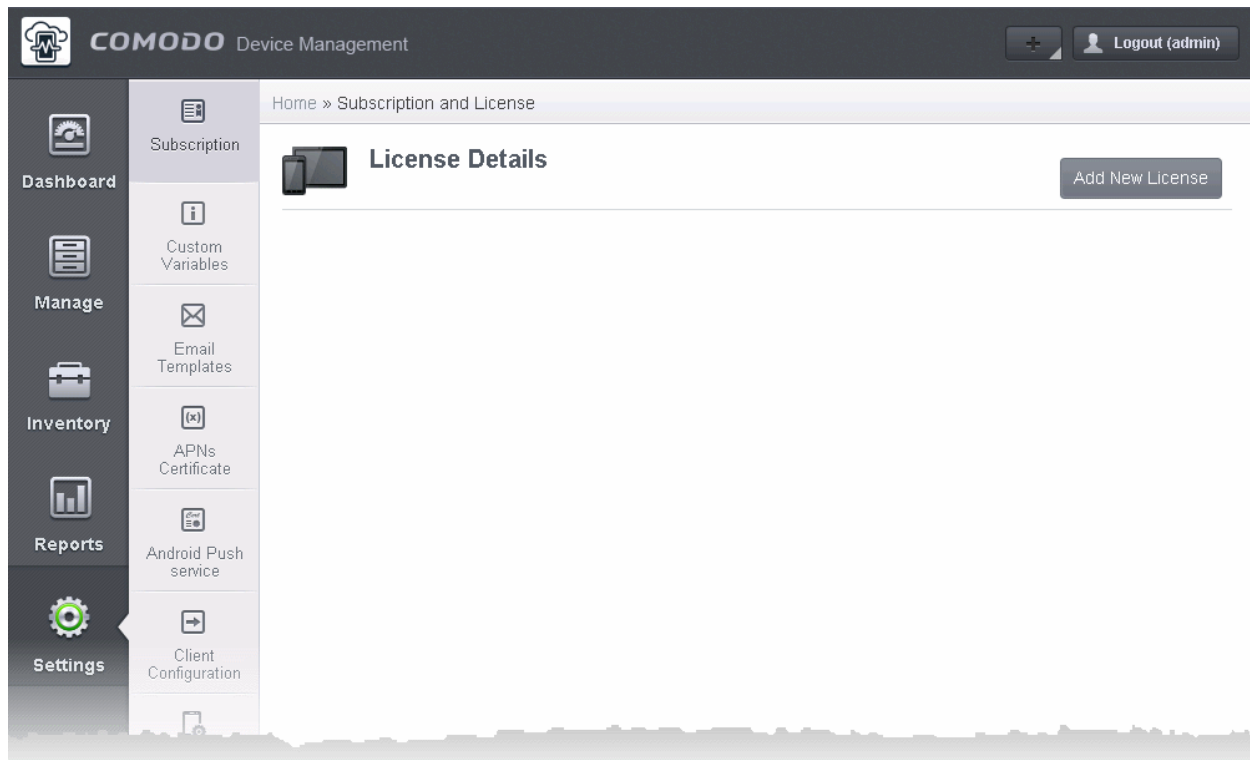
To activate:

- 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:

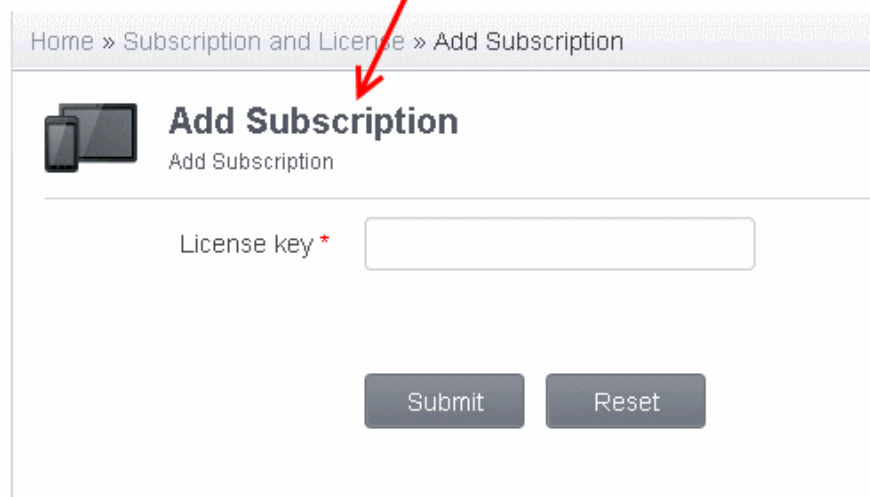
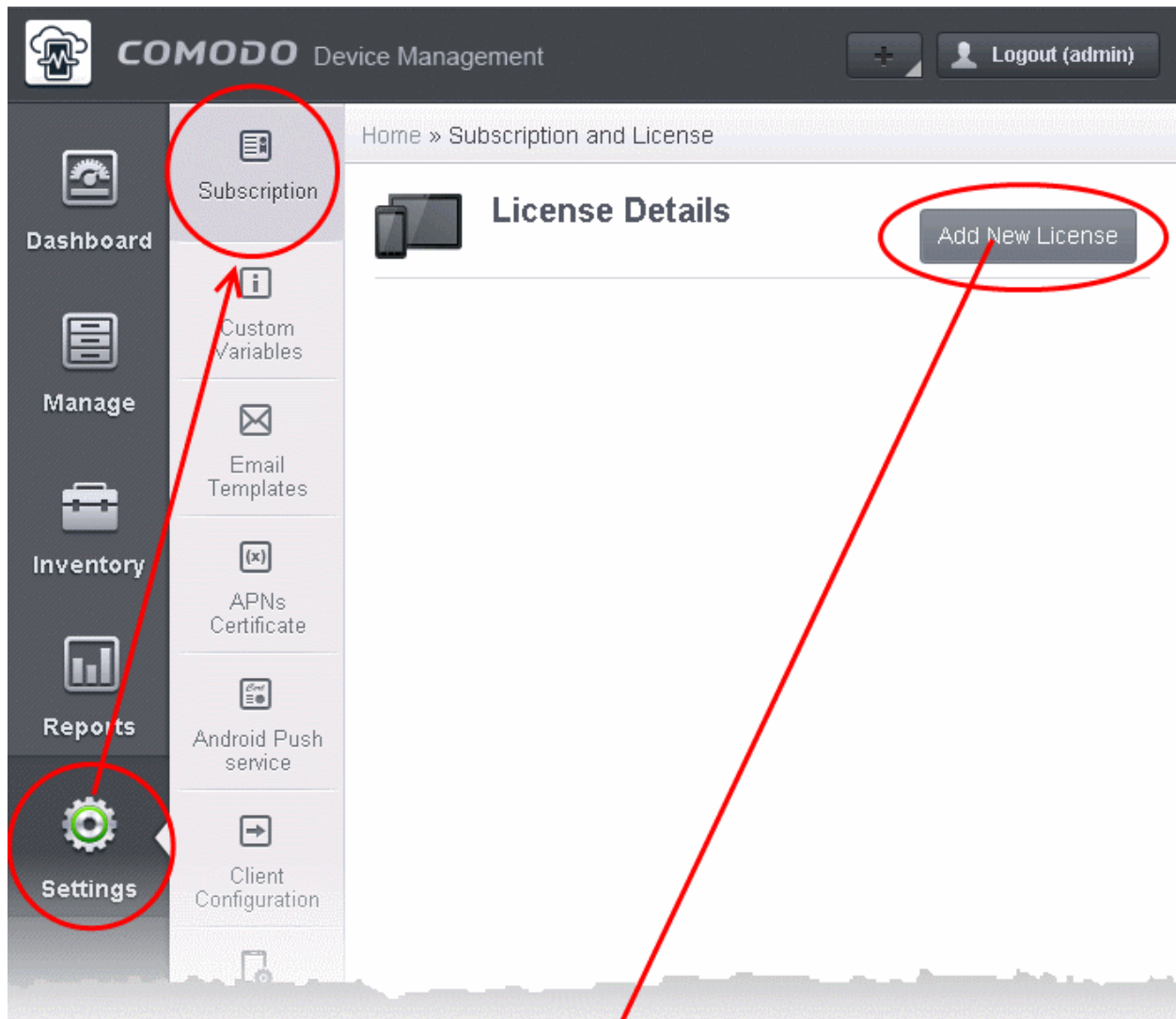


- Login using the following credentials: Username: admin Password : admin
- You can (and should) change these to a unique username and strong password at any time *after* license activation. To do this, log in, click 'Inventory' > 'Users' then click on the user named 'Admin'. Next, click the 'Update' 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 license key at the 'Subscription and License' screen. The subscription ID and license key can be found in your CDM confirmation email.



- Click 'Settings' and then the 'Add new license' button in the 'Subscription and License' screen.




- Enter the license key and click 'Submit'.

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.

Home » Subscription and License

License Details

[Add New License](#)

 Will expire in 1281 day(s)

Subscription ID	201412181247540200
License key	70422a7-21b-43a4-88b-42d81f8148
Max. Users	100
Organization	ABC Company
Licensed to	John Smith
Free	No
Active	Yes
Valid From	2014-12-18T12:47:54+02:00
Expires	2018-12-18T12:47:54+02:00
Time check	2015-06-15T14:02:15+03:00
License Registered at	2015-06-15T14:02:15+03:00

The next step is to configure the SMTP settings.

Step 7 - Configuring SMTP Settings

CDM sends automated emails to administrators and end users at various events like enrollment of a new user/administrator, sending tokens to users for enrolling their devices and so on. The SMTP settings interface allows the administrator to specify the SMTP server to be used by CDM to send those notification emails.

Home » SMTP settings

SMTP settings

Specify the settings for SMTP

Host of SMTP

Port of SMTP

Use auth in SMTP

Secure type in SMTP

Login for SMTP

Password for SMTP

From email

From name

Save

- Complete the form and click 'Save'. For more details on the SMTP settings, refer to our admin guide at <https://help.comodo.com/topic-214-1-519-8083-Configuring-SMTP-Settings.html>

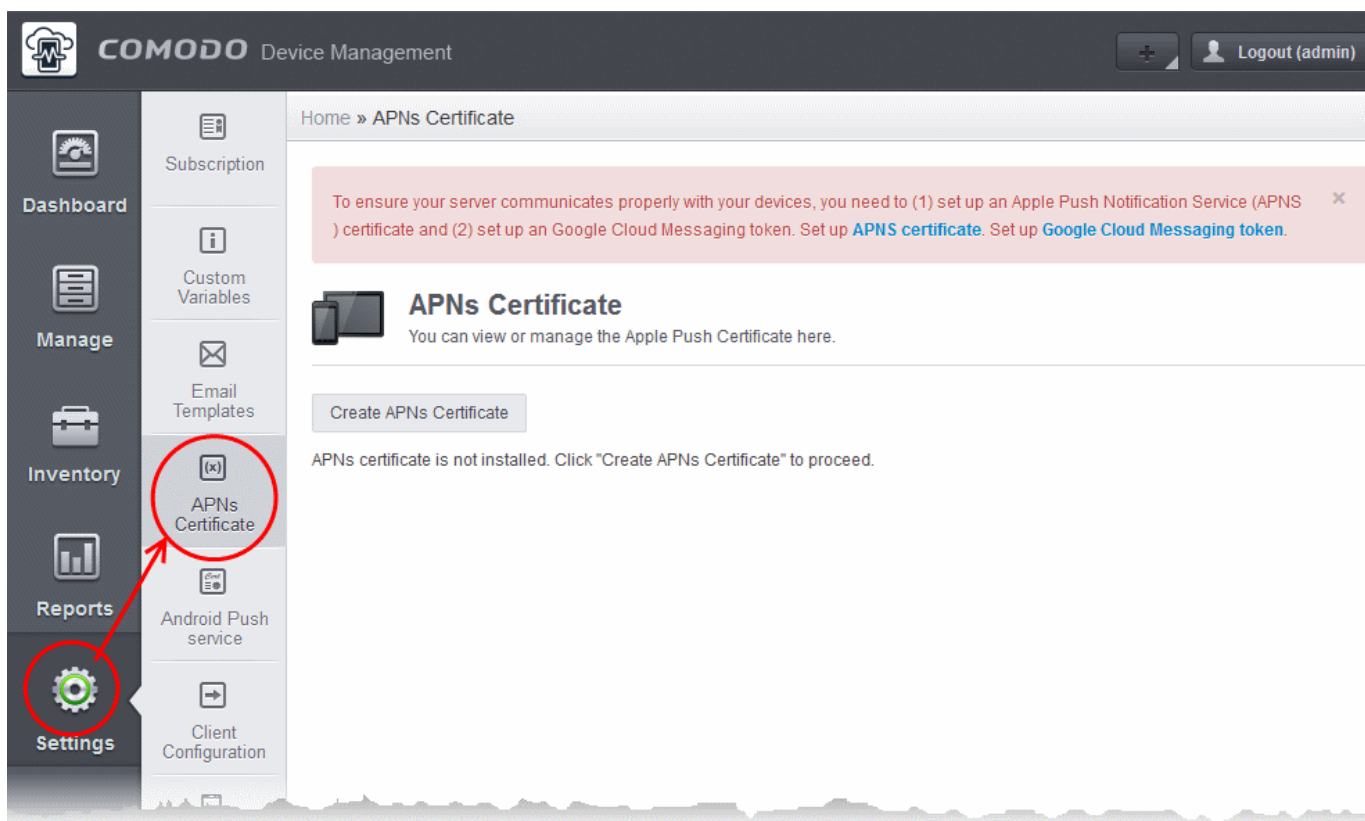
For your first task now that setup is complete, we advise you to configure Apple Push Notification.

Step 8 - 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 - Generate your PLIST

- In the CDM 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):

COMODO Device Management

Home » APNs Certificate » APNs certificate generation

To ensure your server communicates properly with your devices, you need to (1) set up an Apple Push Notification Service (APNS) certificate Messaging token. Set up [APNS certificate](#). Set up [Google Cloud Messaging token](#).

Generation of APNs Certificate

Here you can generate certificate that will be used for Apple Push Notification service. (signed automatically by Comodo)

Country Name *

Email Address *

State or Province Name *

Locality Name (eg, city) *

Organization Name *

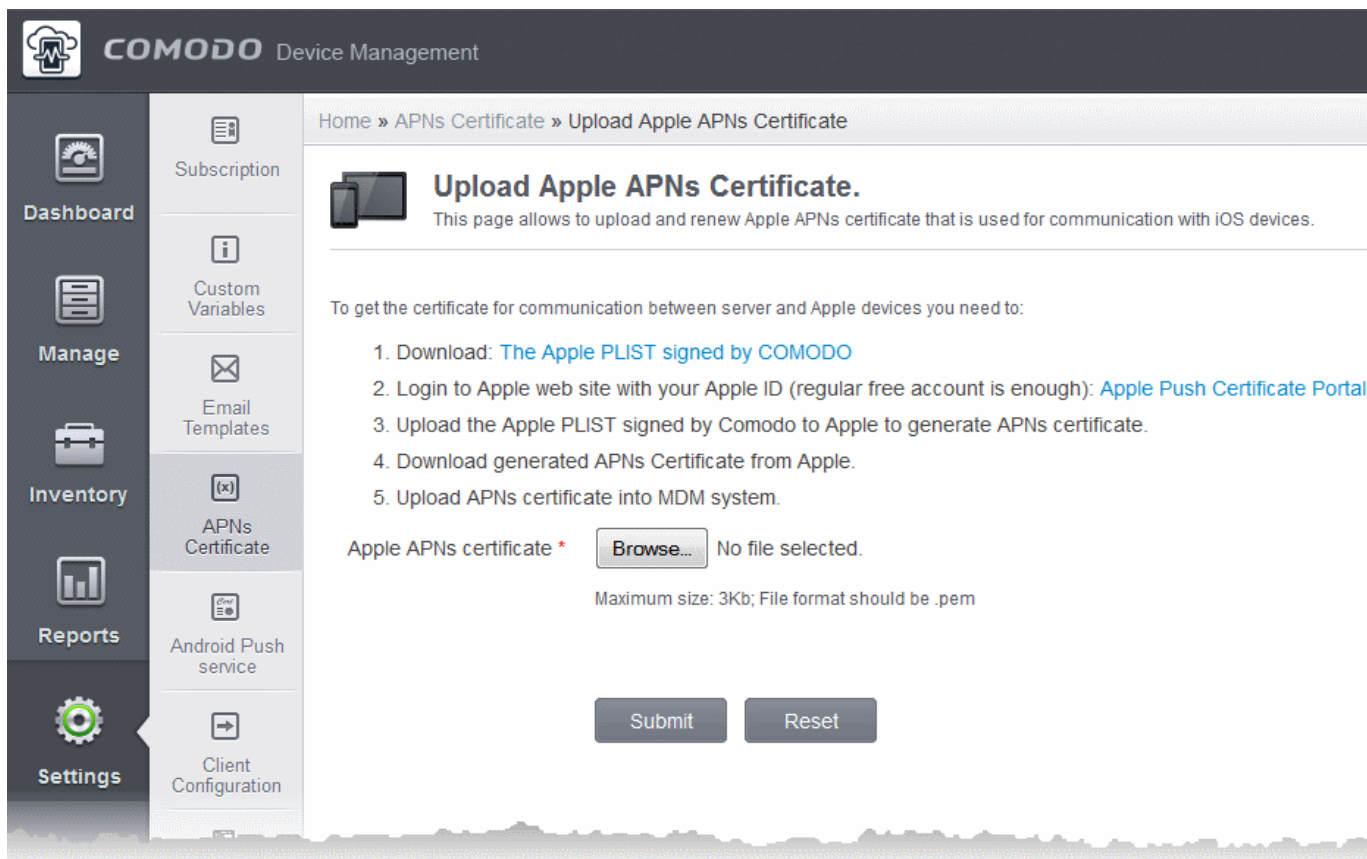
Organizational Unit *

Organizational Unit Name (eg, section)

Common Name *

(e.g. server FQDN or YOUR name)

- Complete all fields marked with an asterisk and click 'Submit'. This will send a request to Comodo 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>.

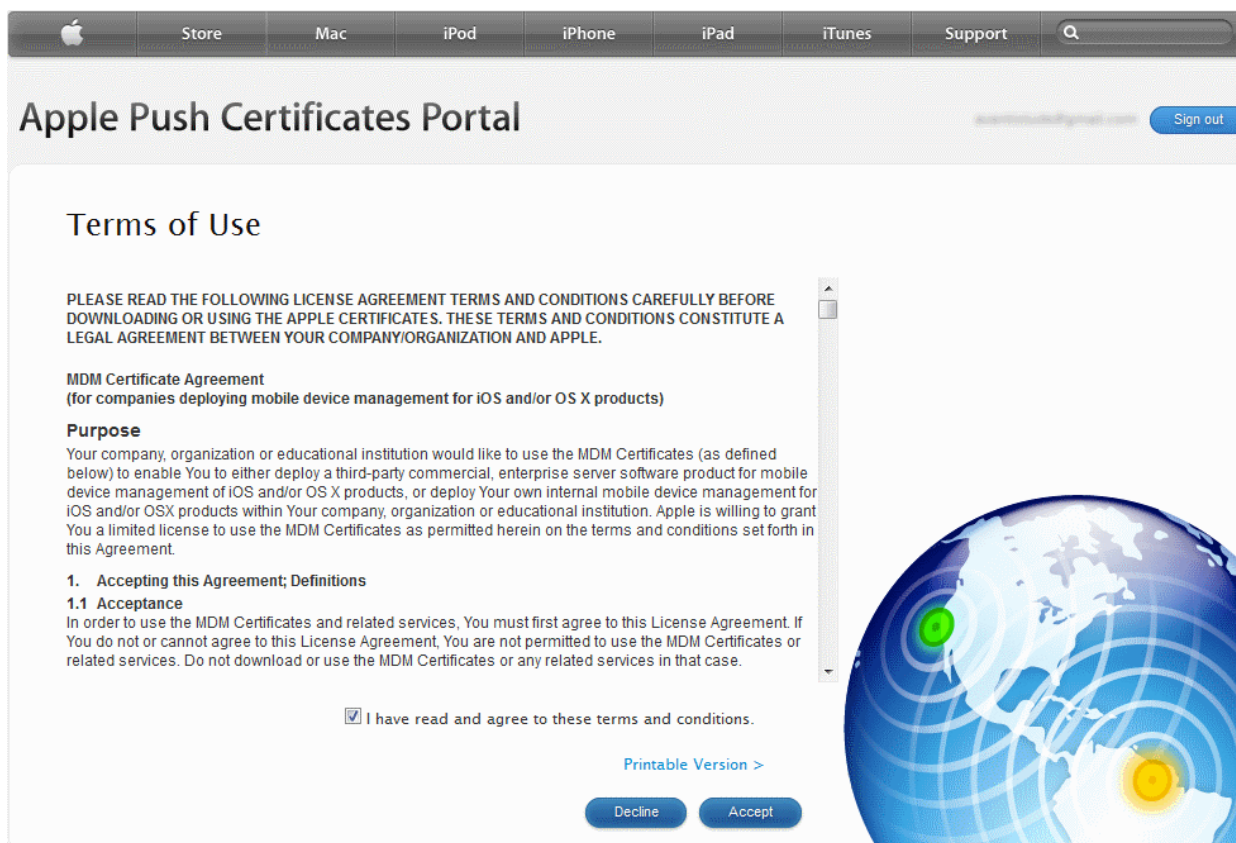
- Once logged in, click 'Create a Certificate'. You will need to agree to Apple's EULA to proceed.



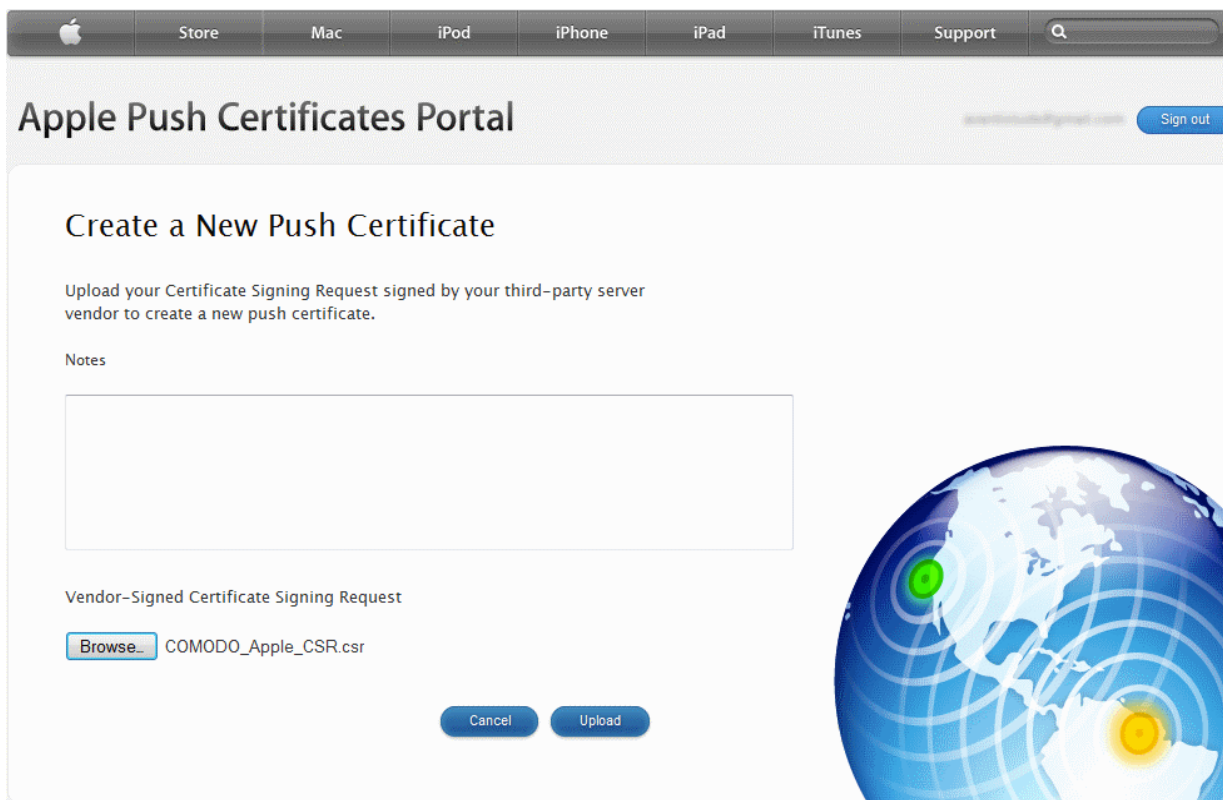
- On the next page, browse to the location where you stored 'COMODO_Apple_CSR.csr' and click 'Upload'.



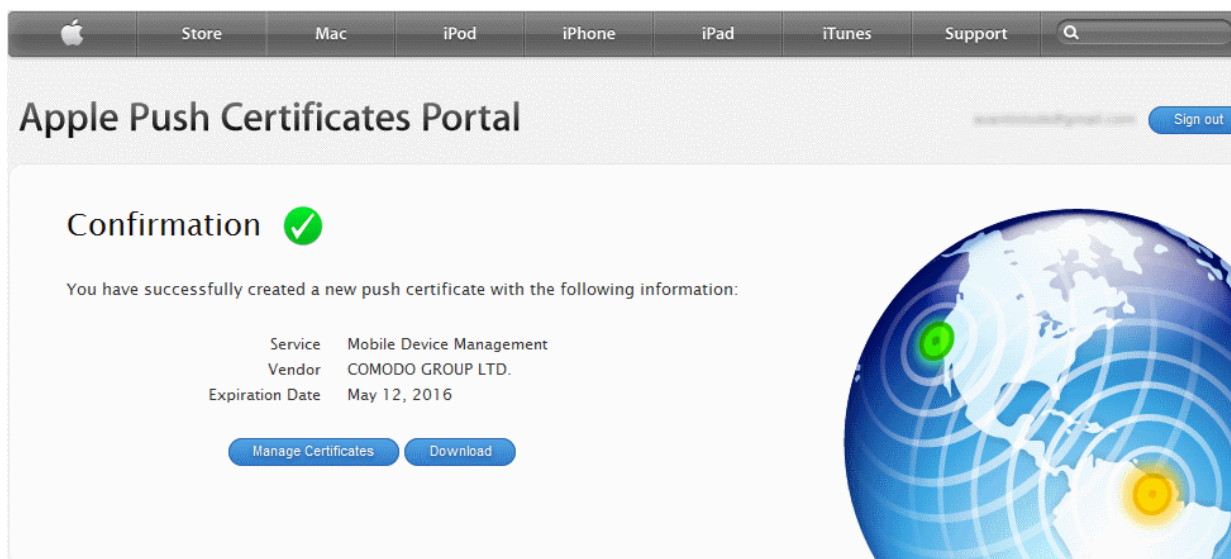
You will need to agree to Apple's EULA to proceed.



- On the next page, click 'Browse', navigate to the location where you stored 'COMODO_Apple_CSR.csr' and click 'Upload'.



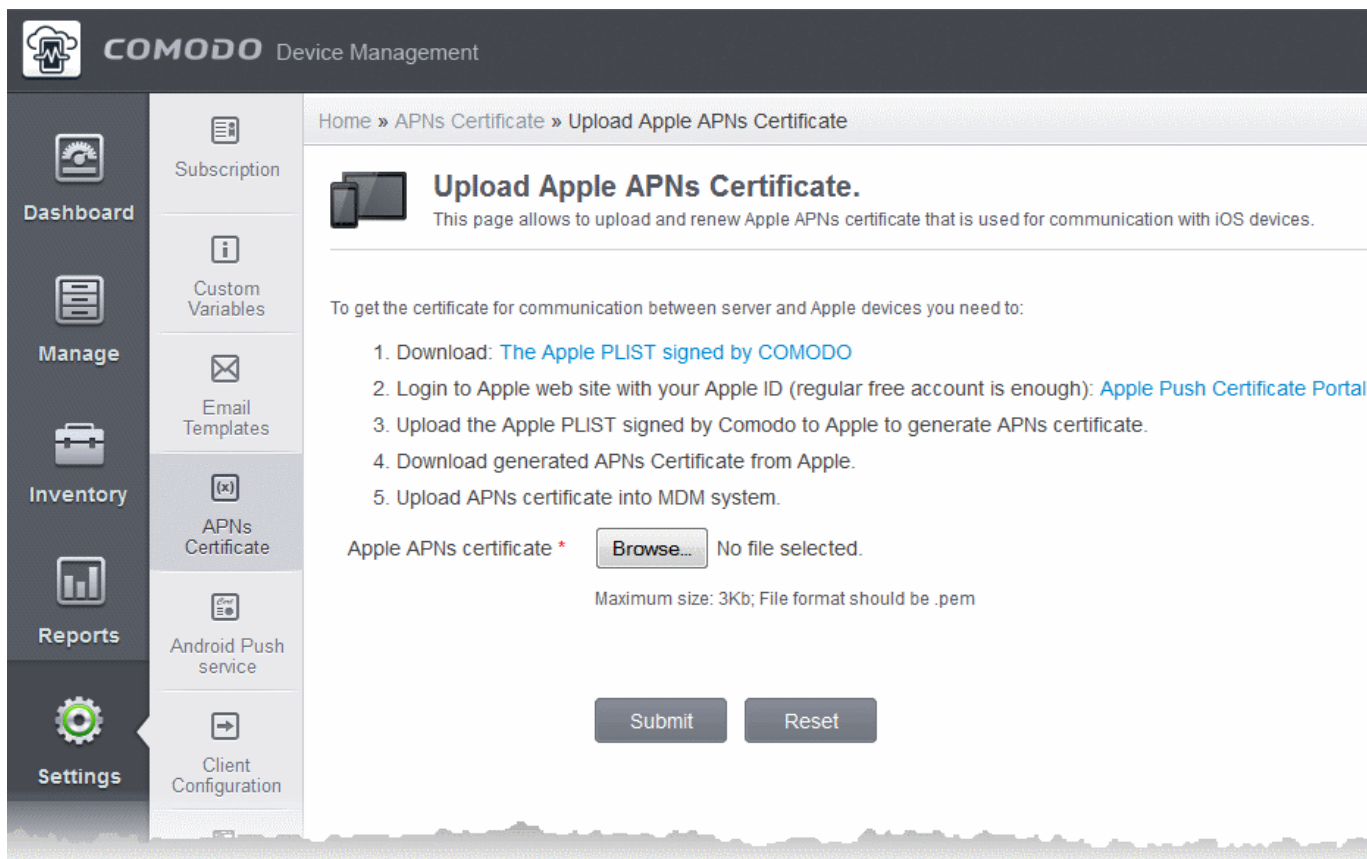
Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:



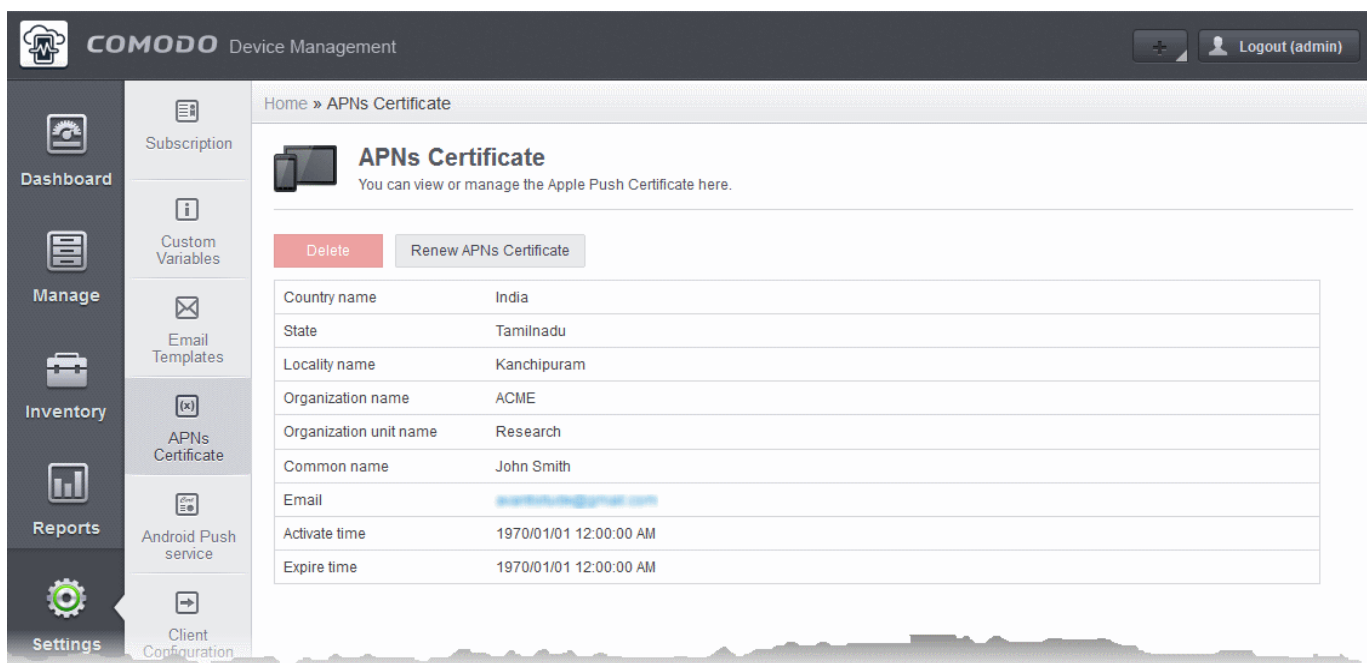
- Click the 'Download' button and save the certificate to a secure location. It will be a .pem file with a name similar to 'MDM_COMODO GROUP LTD_Certificate.pem'

Step 3- Upload your certificate to CDM

- Next, return to the CDM 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:



Your CDM server 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.

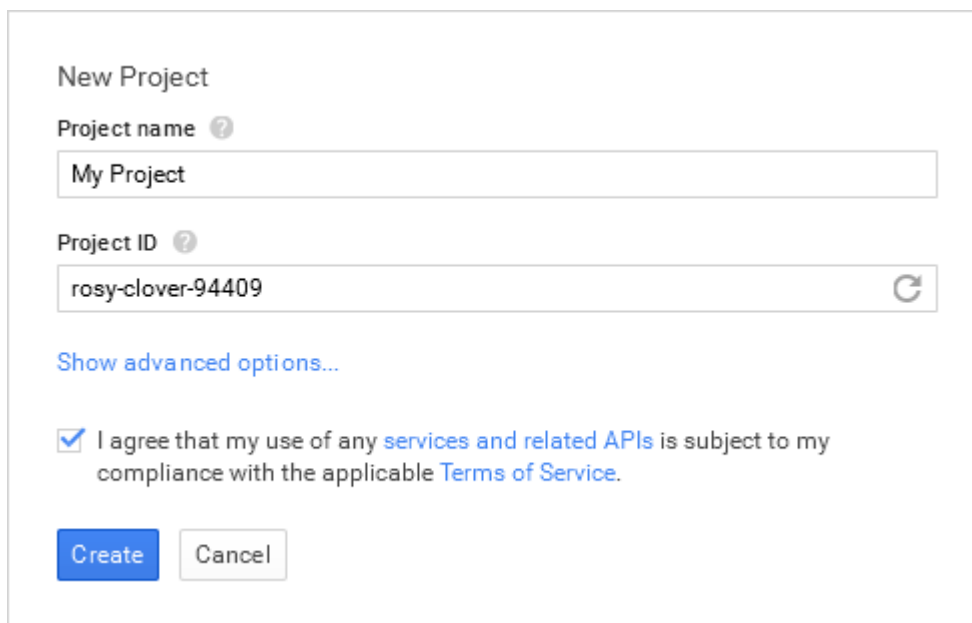
- To renew your APN Certificate, click the 'Renew APN Certificate' button.
- To remove the certificate for generating a new APNs certificate, click the 'Delete' button.

Step 9 - Configuring Google Cloud Messaging (GCM) for Android

Your CDM server needs Google Cloud Messaging token for communicating with the managed Android Devices. Comodo Device Manager ships with a default API token which is hardcoded and not visible in the interface. However, you can generate a unique Android GCM token that can be uploaded to CDM portal. To generate a GCM token, you must have created a Mobile Backend Project at <https://console.developers.google.com>. Please follow the steps given below to create a project and upload a token.

- **Step 1** - Login to the Google API Console at <https://console.developers.google.com> and click the 'CREATE PROJECT' button.

Popup will appear where you need to fill project name and project id fields.



New Project

Project name ?
My Project

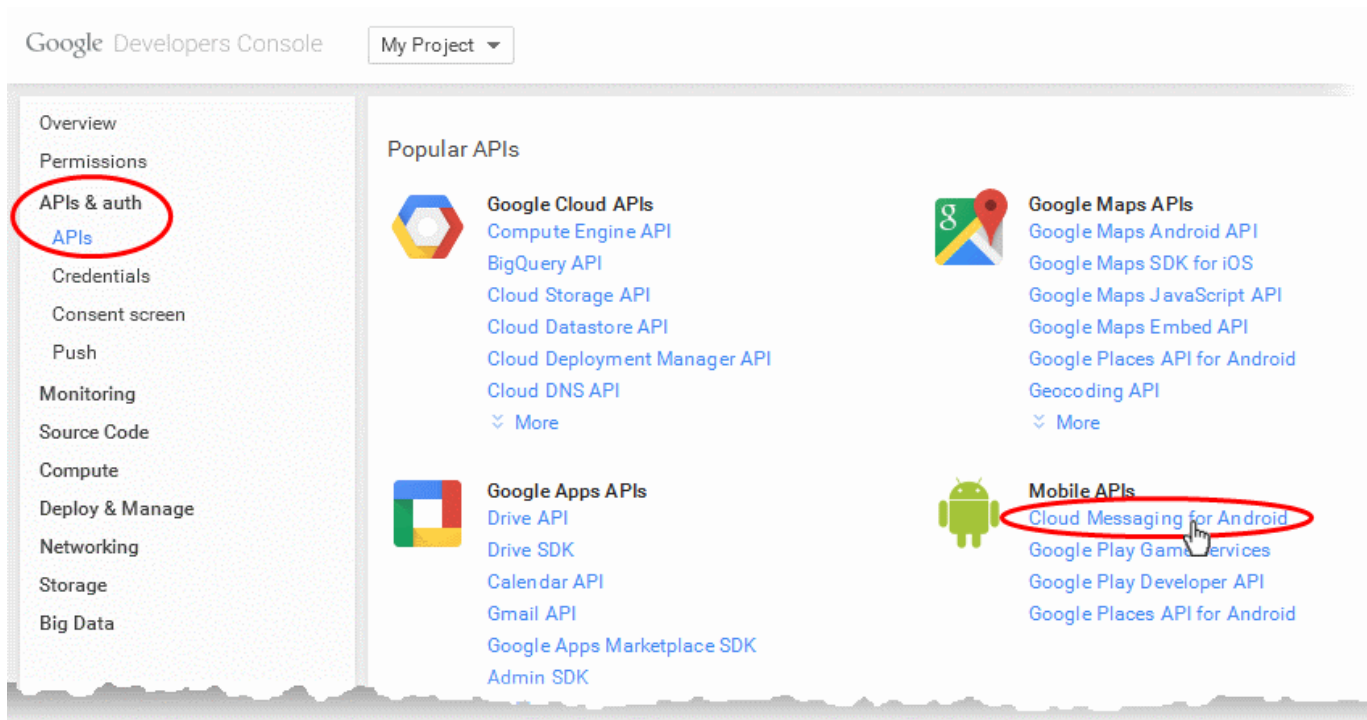
Project ID ?
rosy-clover-94409

[Show advanced options...](#)

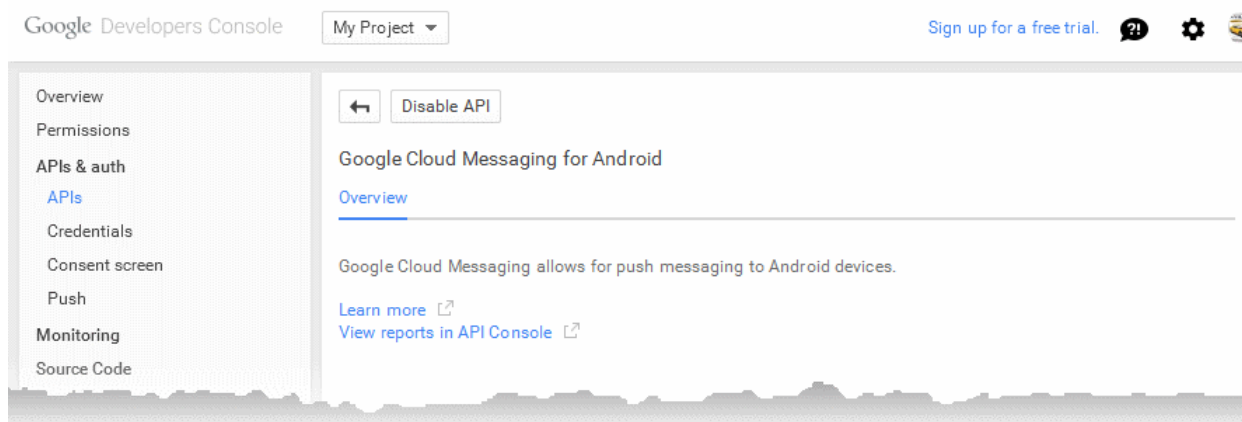
I agree that my use of any [services and related APIs](#) is subject to my compliance with the applicable [Terms of Service](#).


Create Cancel

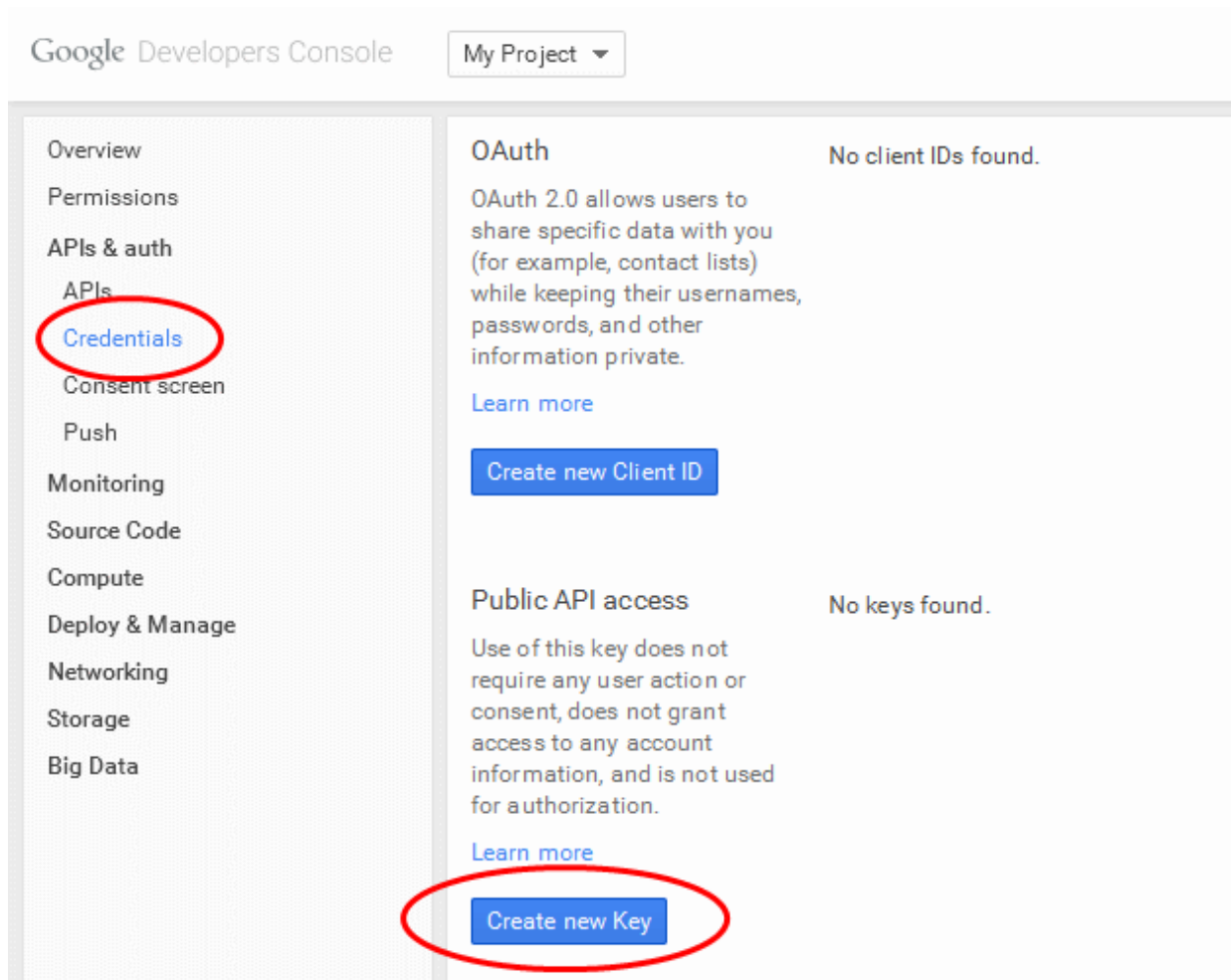
- Enter a 'Project name', choose a 'Project ID'
- Read the Terms of Service by clicking 'Terms of Service' and agree to that by selecting the 'I Agree' check box.
- If you want to choose the data center to be used, click 'Advanced Options' and choose the data center from the drop-down.
- Click 'Create'.
- **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'.



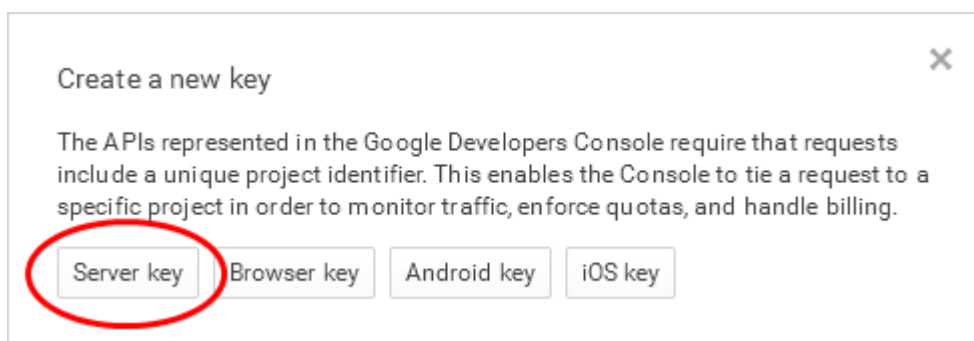
- **Step 4** - Click on "Cloud Messaging for Android" under 'Mobile APIs' in the list of available services.
 - In the next screen, ensure that the service is enabled for the project, else click the 'Enable API' at the top enable the service.



- Click the 'Back' button  at the top to go to the previous screen.
- **Step 5** - Click "Credentials" under "APIs & auth" menu item.



- **Step 6** - Click the 'Create new Key' button under 'Public API Access' and choose 'Server key' in the 'Create a new key' pop-up.



- **Step 7** - Leave the IP Address field blank in the next pop up and click 'Create'.

Create a server key and configure allowed IPs

This key should be kept secret on your server.

Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request's userIp parameter, (if specified). If the userIp parameter is missing, your machine's IP address will be used instead. [Learn more](#)

Accept requests from these server IP addresses (Optional)



One IP address or subnet per line. Example: 192.168.0.1, 172.16.0.0/16, 2001:db8::1 or 2001:db8::/64

Or if you leave this blank, requests will be accepted from any address. Be sure to add IP addresses before using this key in production.

Create

Cancel

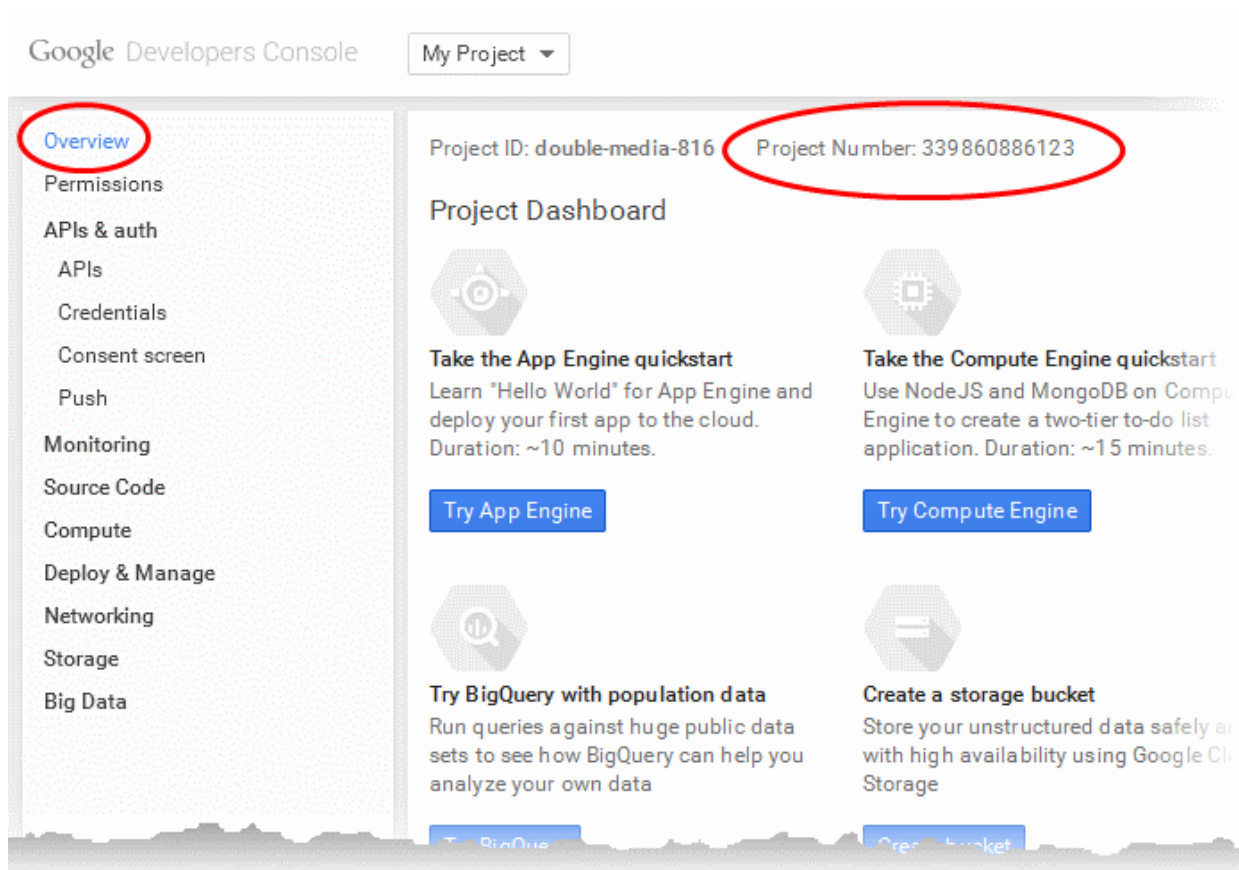
The API Key will be generated and displayed under 'Key for server applications'.

Public API access Use of this key does not require any user action or consent, does not grant access to any account information, and is not used for authorization. Learn more Create new Key	Key for server applications API key:  IPs: Any IP allowed Activation date: May 13, 2015, 9:00:00 AM Activated by:  (you) Edit allowed IPs Regenerate key Delete
---	---

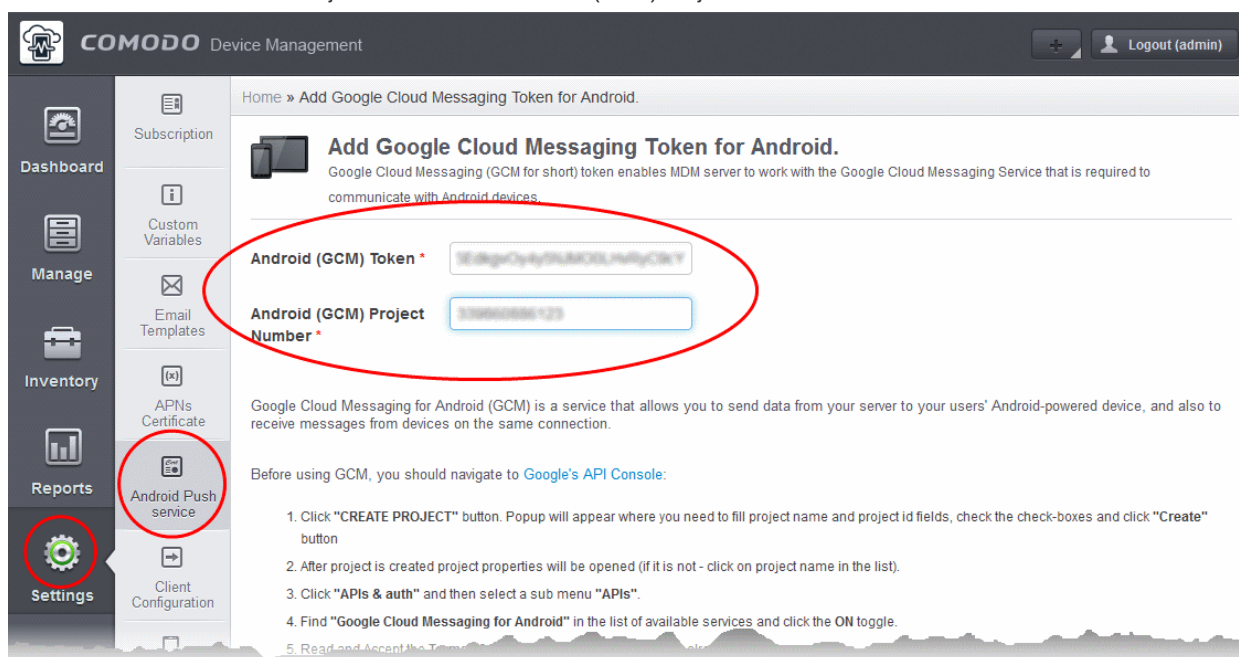
You need the API key and the project number to be entered in the CDM interface.

- Note down the API key in a safe place

To get the project number, return to the project properties interface and click 'Overview' from the left. The Project Number will be displayed at the top of the page.



- **Step 9** - Next, return to the CDM interface and open the 'Add Google Cloud Messaging Token for Android' interface.
 - Paste the API token to 'Android (GCM) Token' field.
 - Enter the Project Number in the Android (GCM) Project Number field.



- Click 'Submit'.

Your settings will be updated. Your CDM server will be now be able to communicate with Android devices.

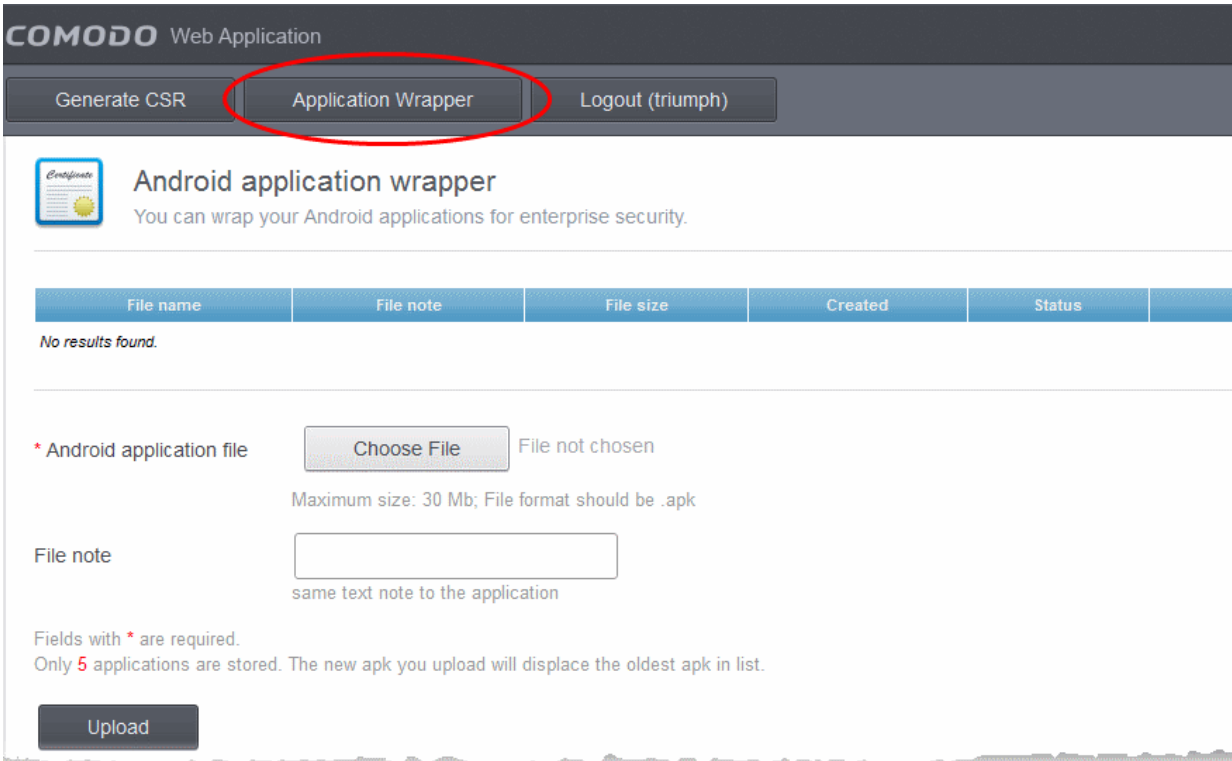
The settings is successfully updated. ✕

Step 10 - Upload your Enterprise/Custom Android App (Optional)

The Comodo Device Manager support portal at <https://mdmsupport.comodo.com> allows the administrator to upload the enterprise or custom Android apps that are to be run isolated in the Android devices enrolled to their account. The CDM server setup in your local network polls mdmsupport.comodo.com periodically and downloads the wrapped enterprise/custom apps that are uploaded for your account and adds the to the 'App Catalog' as 'Mandatory' Apps. The Apps are then pushed automatically to the Android devices enrolled to your CDM server. For more details on the App Catalog, refer to the online help page explaining the 'App Catalog' at <https://help.comodo.com/topic-214-1-519-6129-Managing-Applications.html>.


To upload your enterprise/custom app

- Visit <https://mdmsupport.comodo.com/>
- Login using your Comodo Account Management credentials. This is the username and password you originally created on the CDM application forms and which you should have used while applying for your certificate.
- Click the 'Application Wrapper' tab to open the 'Android application wrapper' interface.



COMODO Web Application

Generate CSR **Application Wrapper** Logout (triumph)

 **Android application wrapper**
You can wrap your Android applications for enterprise security.

File name	File note	File size	Created	Status
No results found.				

* Android application file File not chosen
Maximum size: 30 Mb; File format should be .apk

File note
same text note to the application

Fields with * are required.
Only 5 applications are stored. The new apk you upload will displace the oldest apk in list.

- Click 'Choose File', navigate to the location of the .apk file of the Enterprise/Custom application to be uploaded, select the file and click 'Open'.
- Enter a short description of the application in the 'File Note' text box.
- Click 'Upload'.

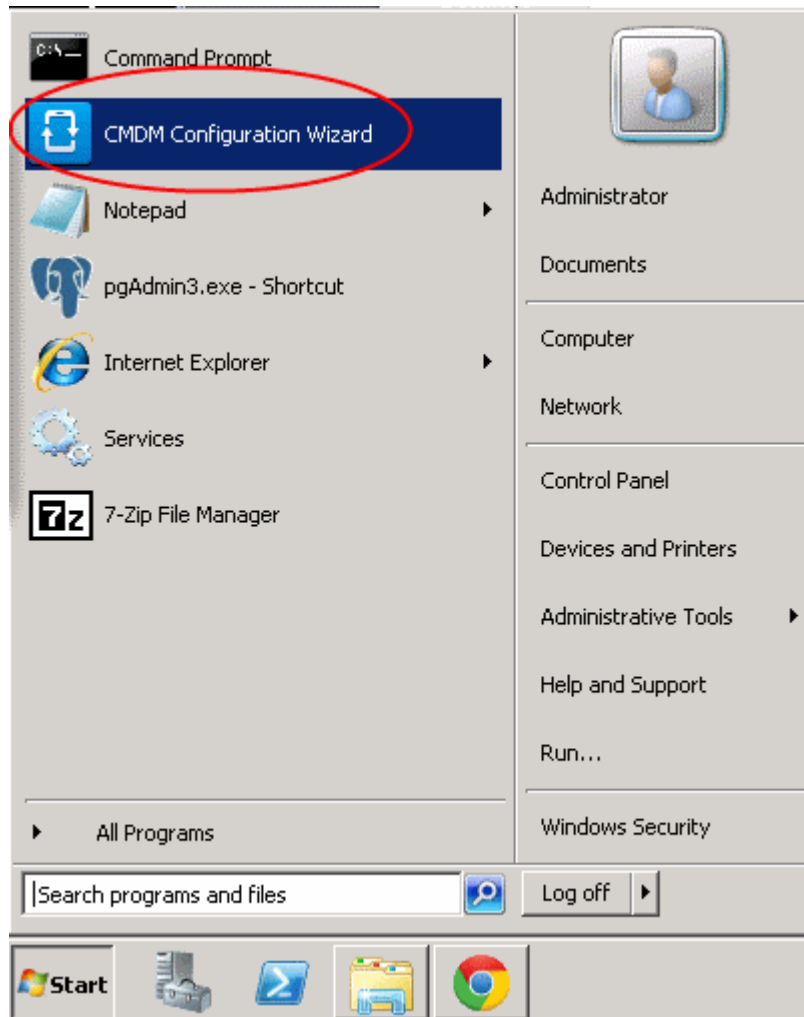
The file will be uploaded, applied with the containment technology and forwarded to the CDM server for adding to 'App Catalog'.

- Repeat the process to upload more number of apps

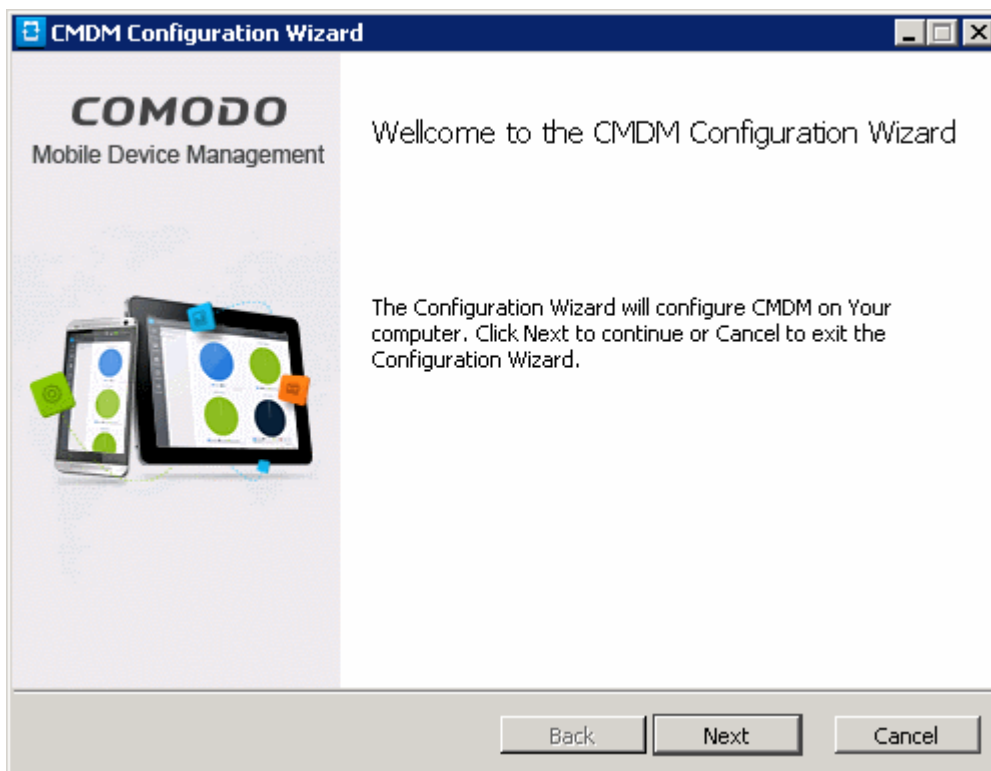
Note: You can have only five applications associated with your account at a time. If a new application is uploaded after the fifth app, the new app will replace the oldest app in the list.

2.Reconfiguring CDM

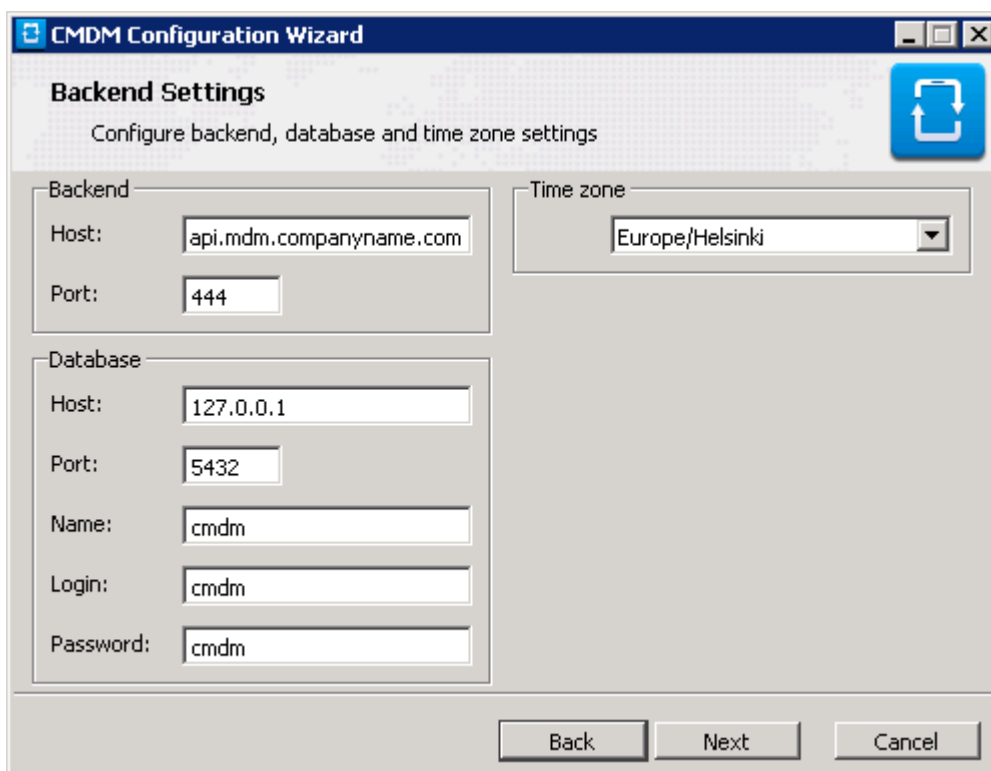
If required, administrators can reconfigure the server backend, frontend and certificate settings at any time using the re-configuration wizard. The wizard can be opened from the start menu of the CDM installation server:

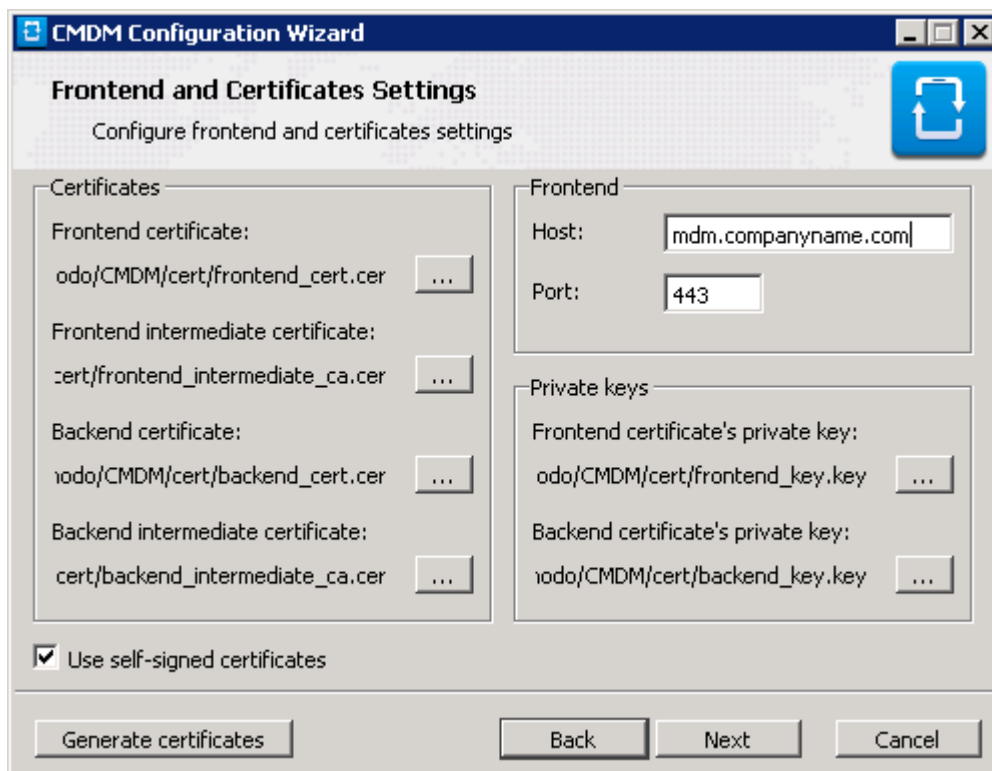


- Click 'Next' in the configuration wizard.

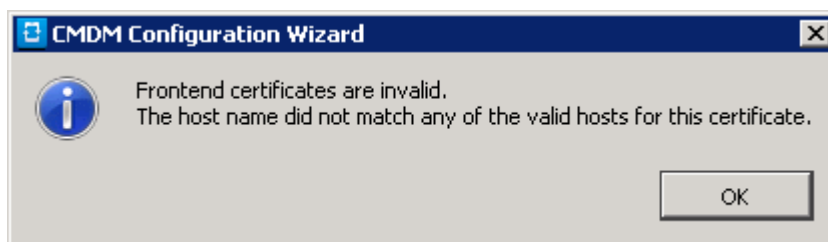


- The wizard uses a very similar interface to the one used during initial configure. Administrators should modify whichever settings they require in the 'Backend' and 'Frontend & Certificates' screens:

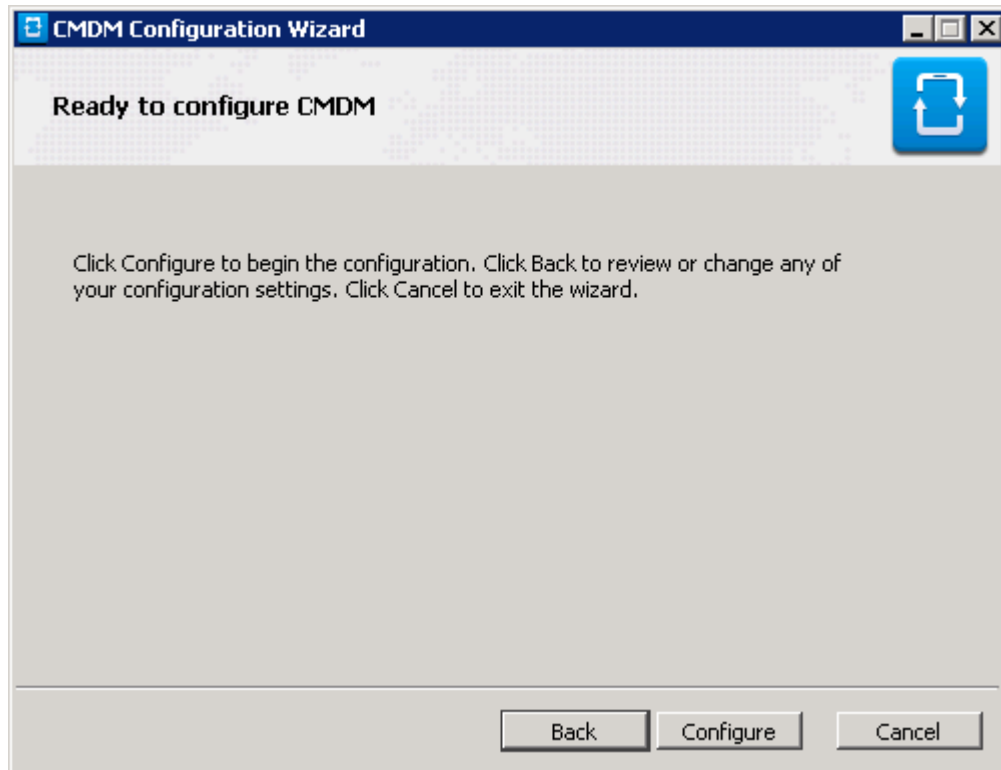




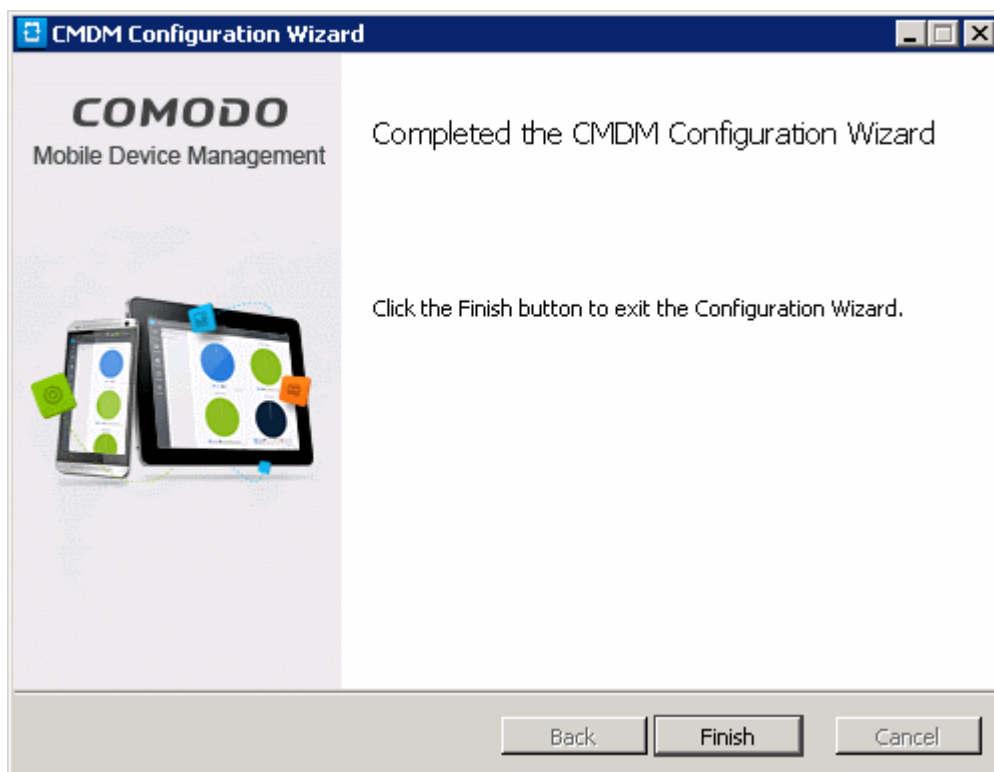
Please make sure that the certificates for the hosts are still valid if you change host details:



- Click 'Configure' in the next dialog, after editing the required parameters.



- After configuration is complete, click 'Finish' to finalize the reconfiguration and exit the wizard.



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>.