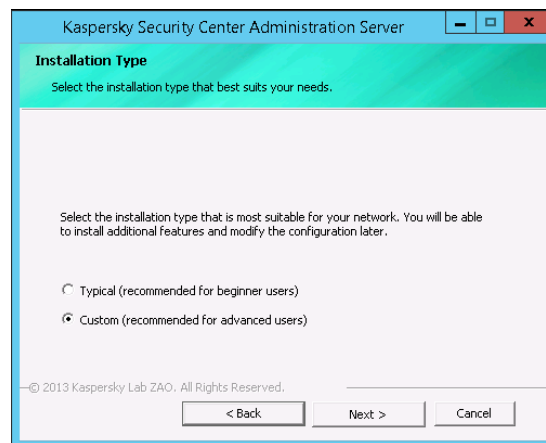


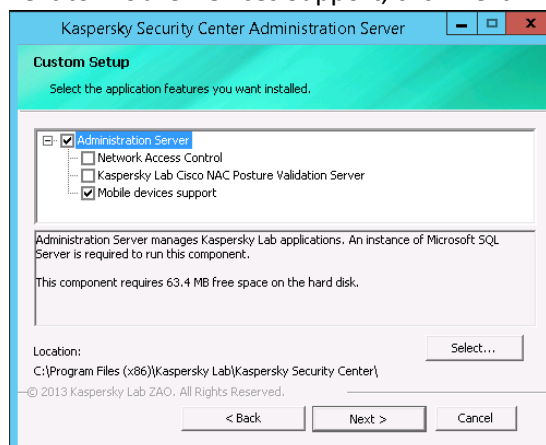
Deploying MDM (Mobile Device Management) in SP1

I. Install KSC

When prompted, select a Custom Installation, as shown.



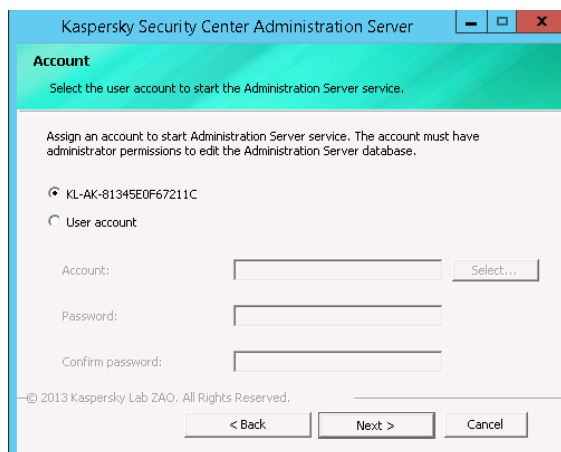
Then, click the checkbox next to Mobile Devices Support, click Next:

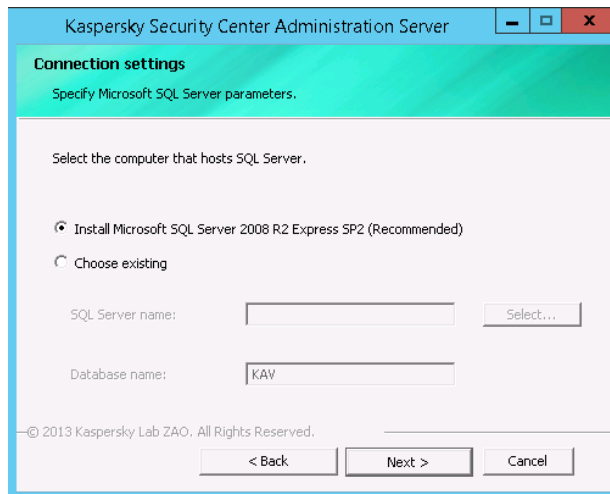
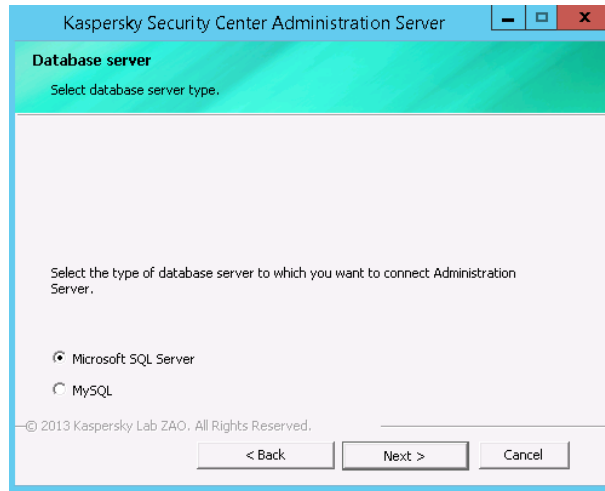


Select network size, click Next:



Unless otherwise required, click Next in each of the next six windows:





Kaspersky Security Center Administration Server

SQL Authentication Mode

Choose Authentication Mode.

Choose the authentication mode you want to use to connect to Microsoft SQL Server. If you select SQL Server Authentication, enter the account and confirm the password.

Microsoft Windows Authentication Mode

SQL Server Authentication Mode

Account:

Password:

Confirm password:

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

Kaspersky Security Center Administration Server

Shared folder

Create a new shared folder or select an existing one.

Shared folders store installation packages and updates for Kaspersky Lab applications. Create a new shared folder or select an existing one.

Create a shared folder

Folder:

Shared folder name:

Select existing shared folder

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

Kaspersky Security Center Administration Server

Connection settings

Specify settings to connect to Administration Server.

Enter the Administration Server ports. Port numbers must be within the range of 1 to 65535.

Port number:

SSL port number:

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

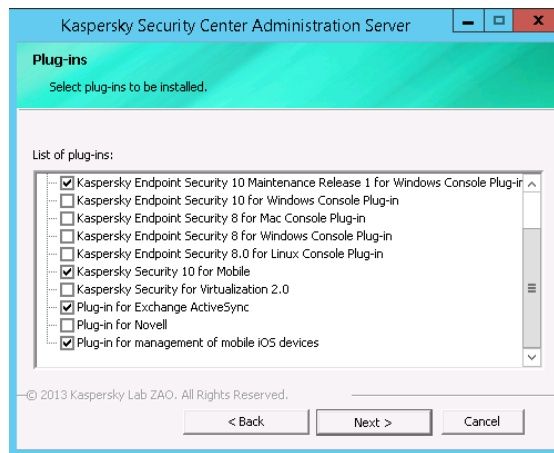
Configure the Administration server address here – this is used in configuring the Network Agent. Click Next to move to the next screen:



Enter in the address that the Mobile Devices connect to the server through, click Next:



In the next screen, click the check next to all the plugins you will need – in this case, we are selecting the items for Mobile support (KSM 10, Exchange ActiveSynch and iOS devices)

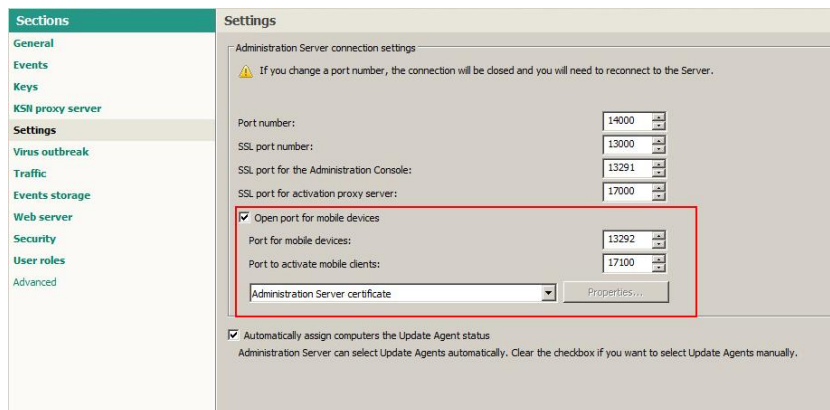


Then click Next and Install to start the installation:

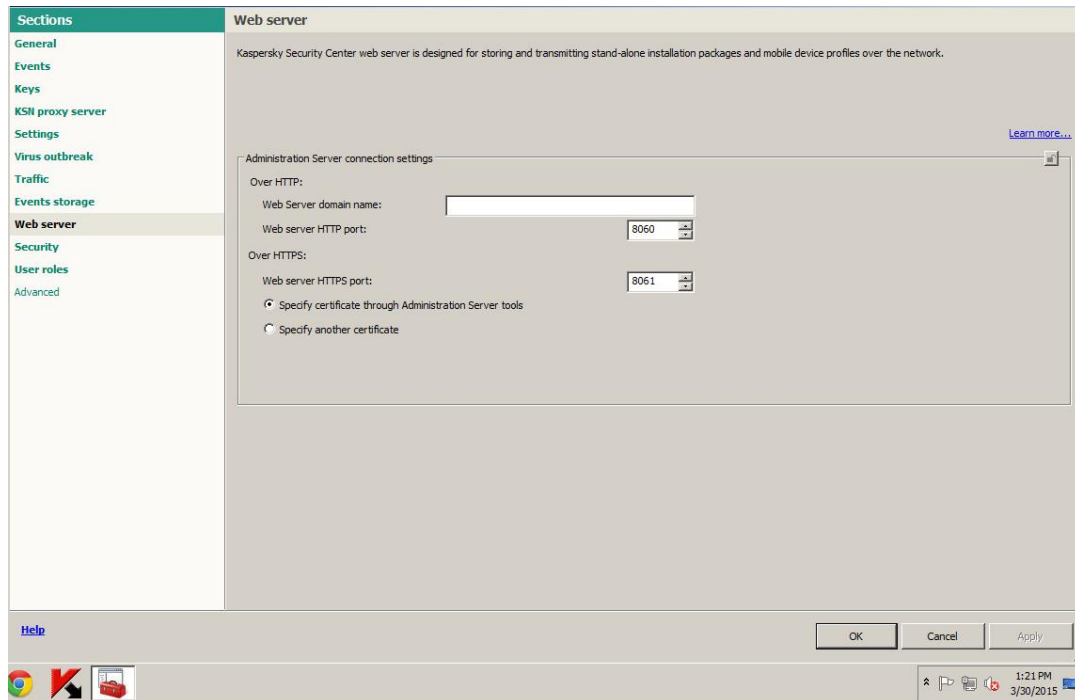
II. Confirm mobile device support and configure KSC if needed

- a. In the KSC, right click on the Administration Server, and select Properties. In this screen, click settings.

Confirm the Open port for mobile devices has been checked and the port numbers are active and editable. (The red outlined area below)



Open the KSC Admin Console and connected to the server, right click on the Administration server and click on the Web server node in the left pane:



- a. In the Web Server domain name, type the IP address of the external connection to your network (the Internet facing connection for your KSC web server)

Click OK to exit the screen.

III. Connect KSC to GCM (Google Cloud Messaging)

The Kaspersky Security Center connects to GCM to Android devices to provide the ability to perform tasks on them such as data wiping, locating, etc.

Note that there will be a need to open ports for the KSC Administration Server to connect to the Google Cloud Messaging services or GCM

The ports are:

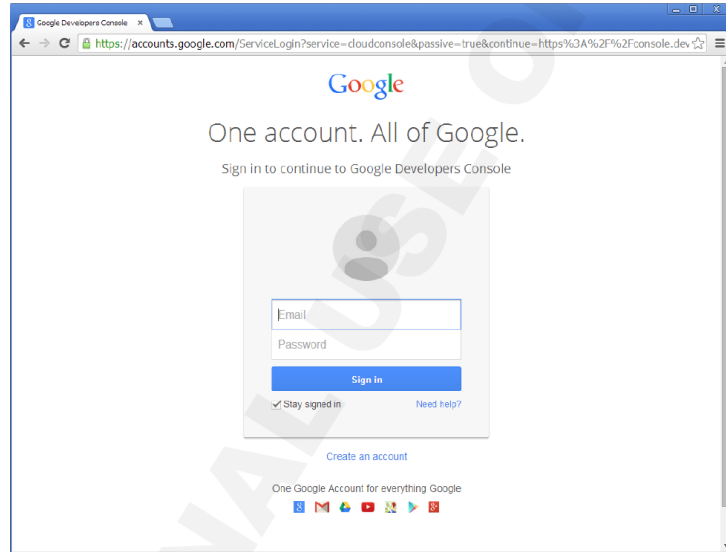
5228	outbound	android.apis.google.com	for client management
5229	outbound	android.apis.google.com	for client management
5230	outbound	android.apis.google.com	for client management
443	outbound	android.apis.google.com, google.com	

(Please see the appendix for illustrations of ports/connections needed)

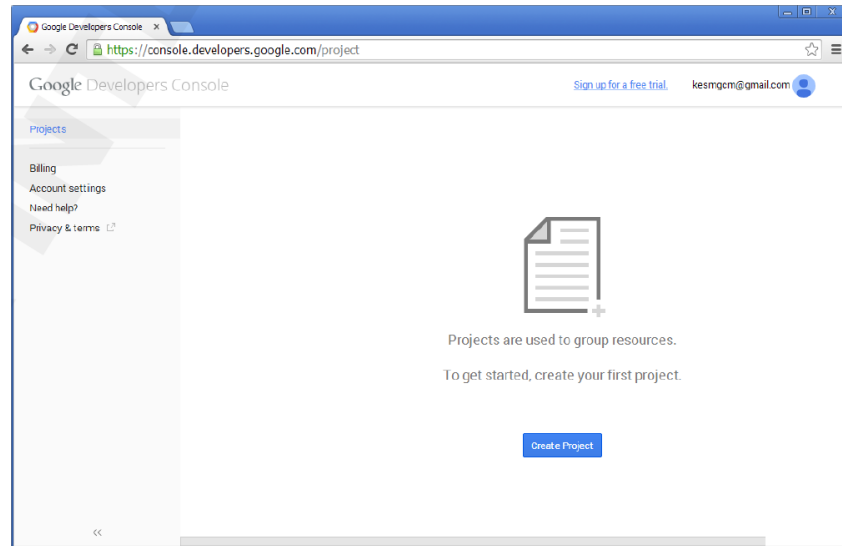
GCM – Defining a Project at Google

Create a mobile device management project in the Google Developers Console.

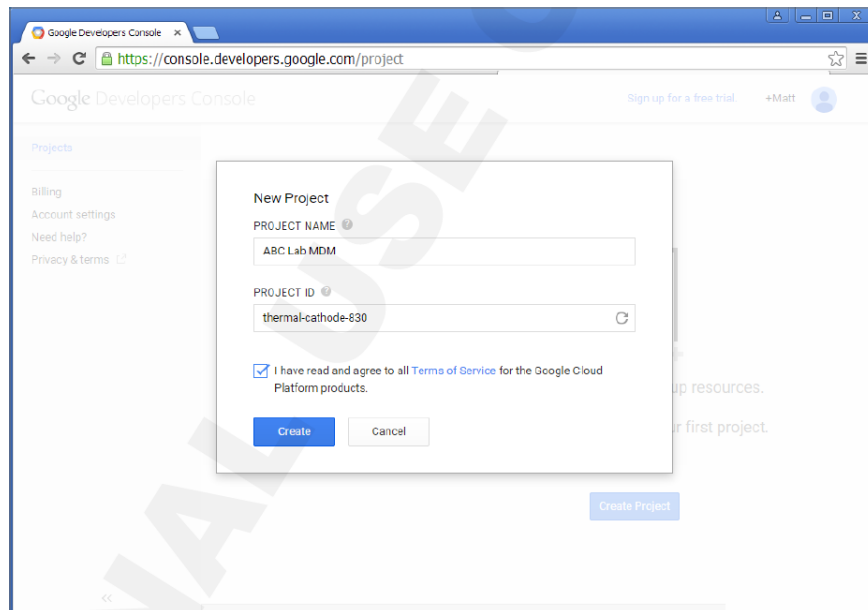
Open a browser and got to <https://console.developers.google.com/project>



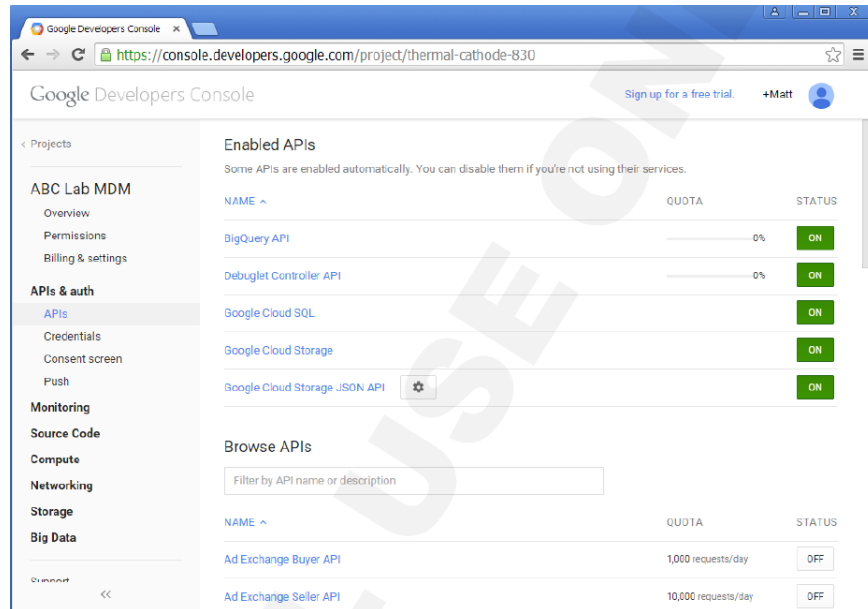
- b. Log in with a Google account and in the next screen, click Create Project in the middle of the screen:**



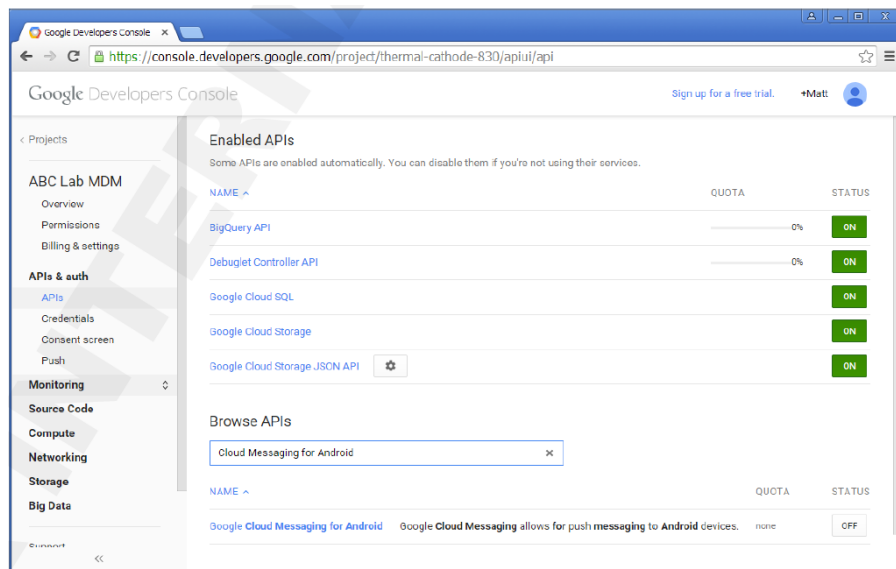
- c. Enter a name in the PROJECT NAME field, and click the Terms of Service checkbox, and click Create:



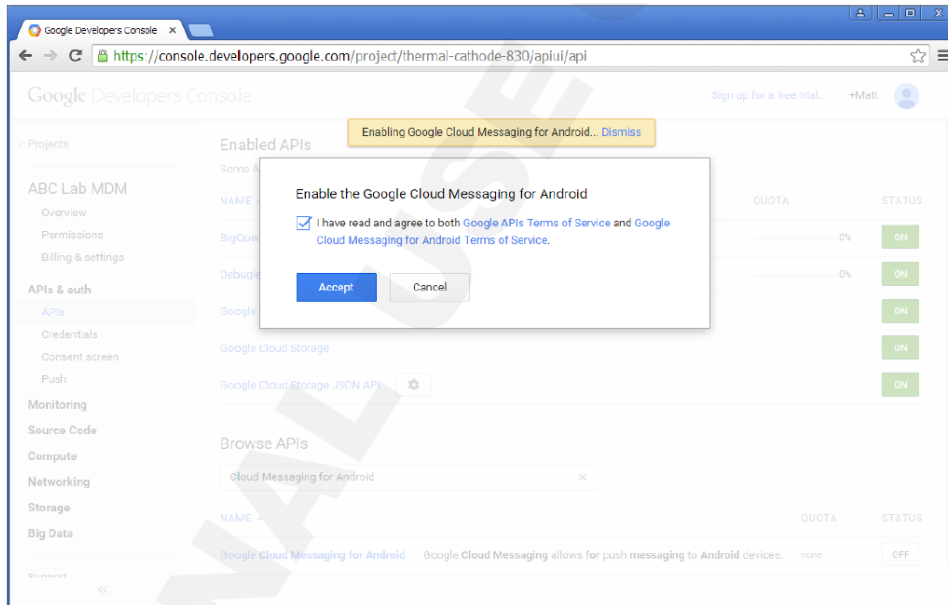
- d. Wait for the project to be created, then click on the APIs and auth link:



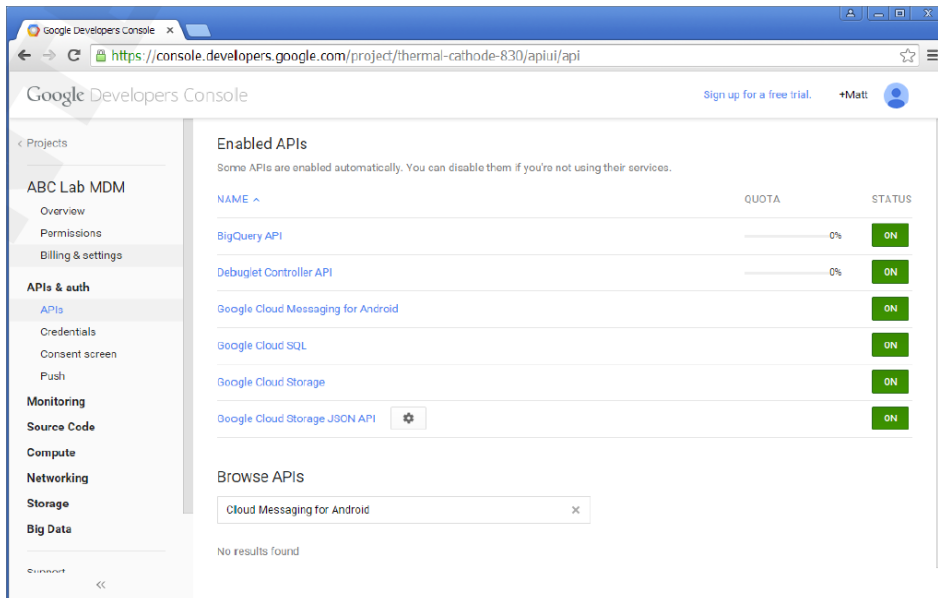
- e. Click on the APIs header, and in the Browse APIs field, type Google Cloud Messaging for Android.



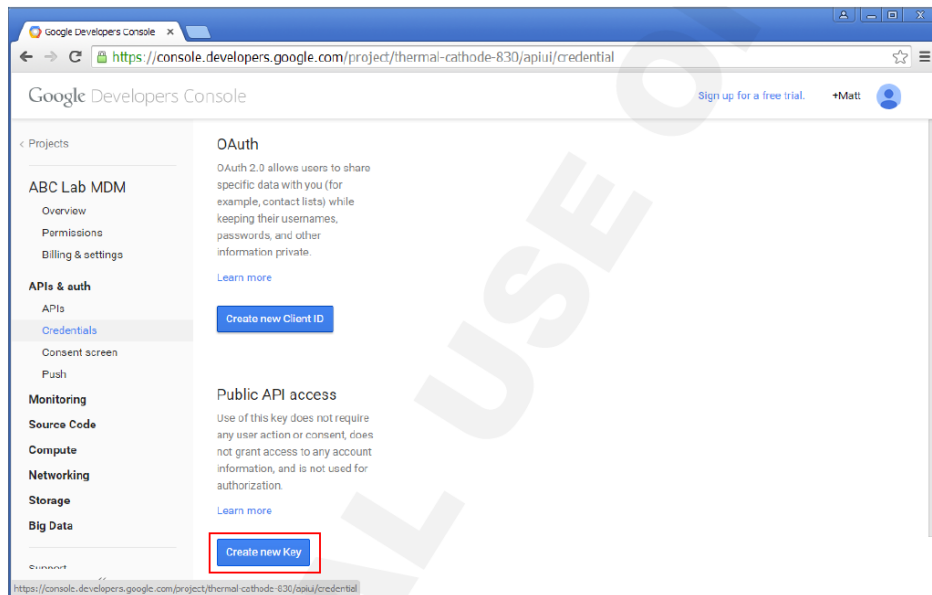
When located, change the status of Google Cloud Messaging for Android from Off to On, and accept the terms of service with the checkbox:



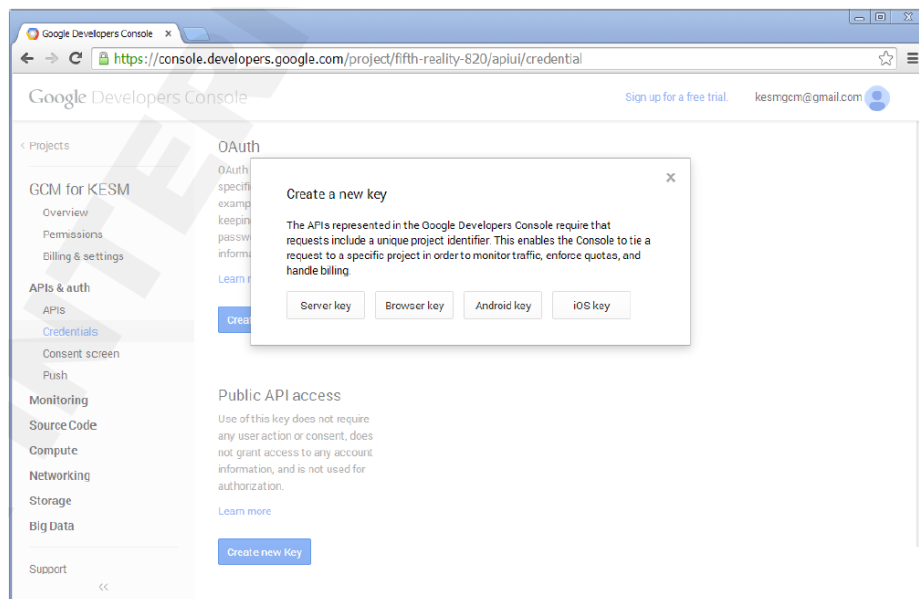
- f. **Confirm the Google Cloud Messaging for Android record is showing in the Enabled APIs list and its status is ON:**



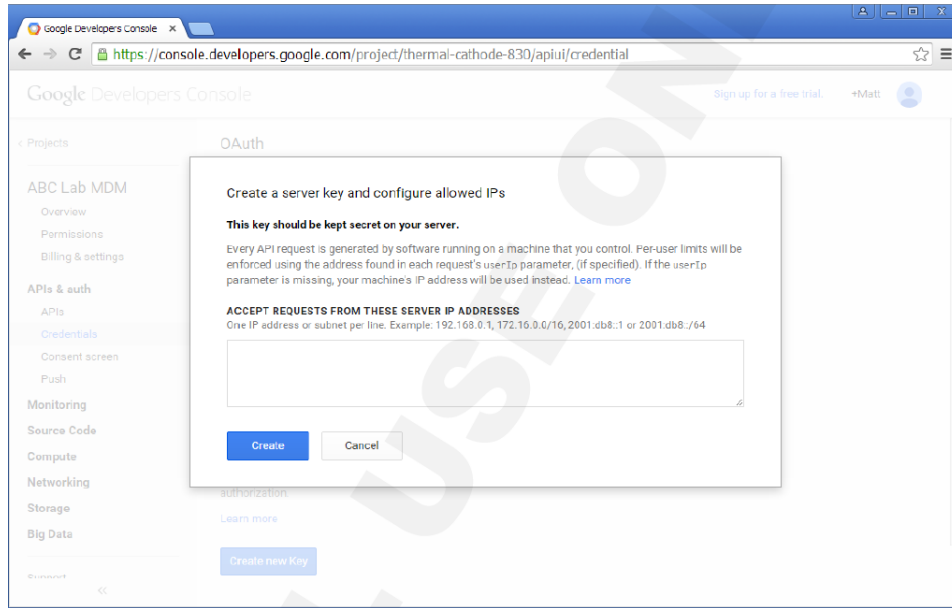
- g. Next, on the left, select the Credentials node under APIs and auth and in that window, click Create new key (outlined in red below)



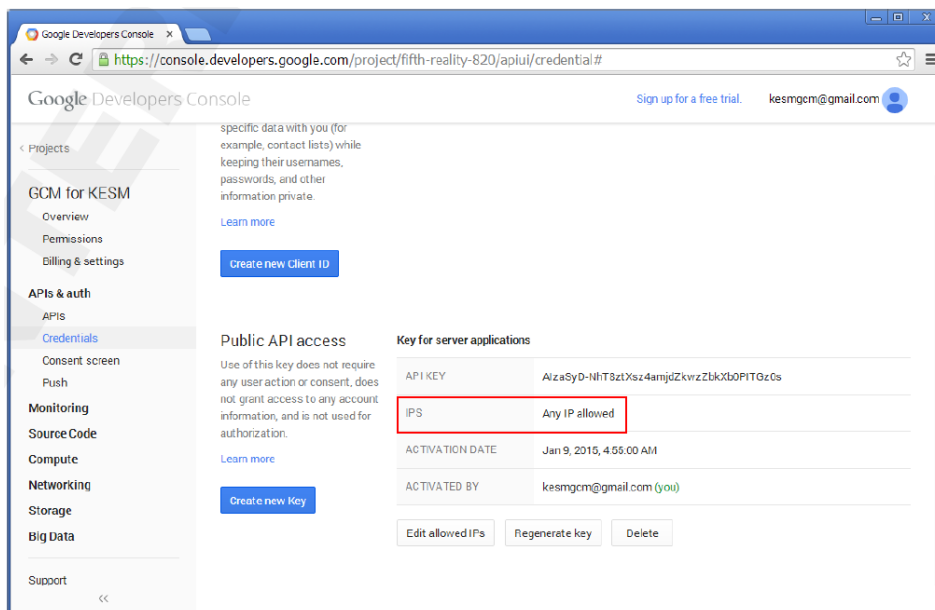
- h. In the next dialog box, click Server key:



i. Then in the next screen, click Create:

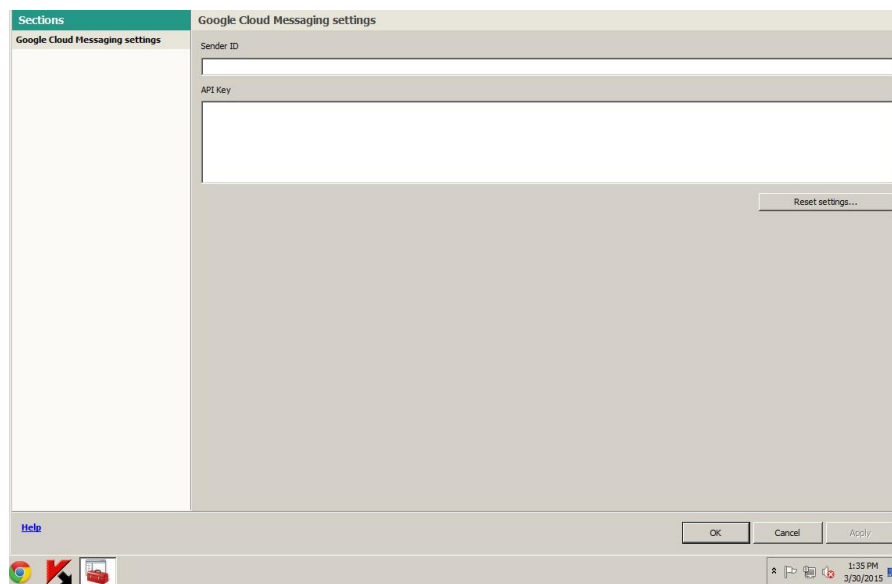


j. Once the key is created, make sure it is set to IPS – Any IP allowed, as shown below. Also – keep this browser window open, as there is data needed to configure the KSC here.

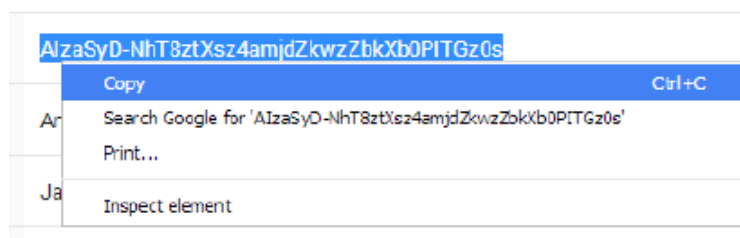


Configuring GCM on the KSC server

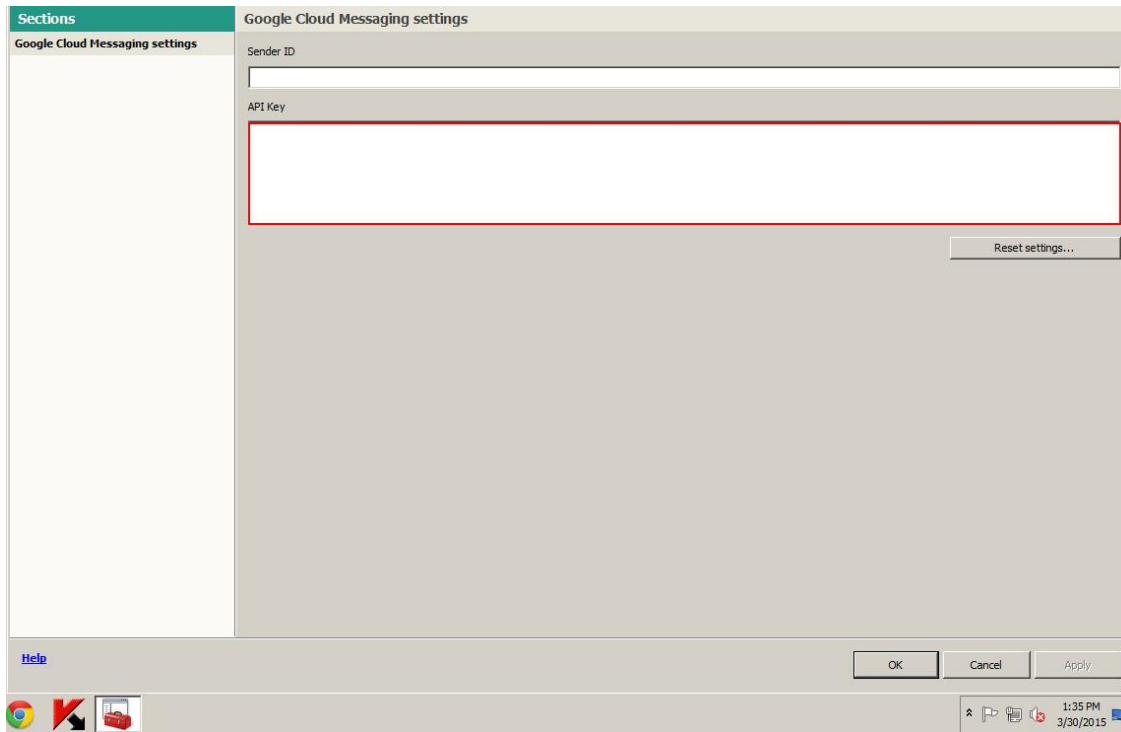
In the left hand pane, expand the Mobile Device Management node. Right click on the Mobile devices heading, and click Properties – this is where we configure Google Cloud Messaging:



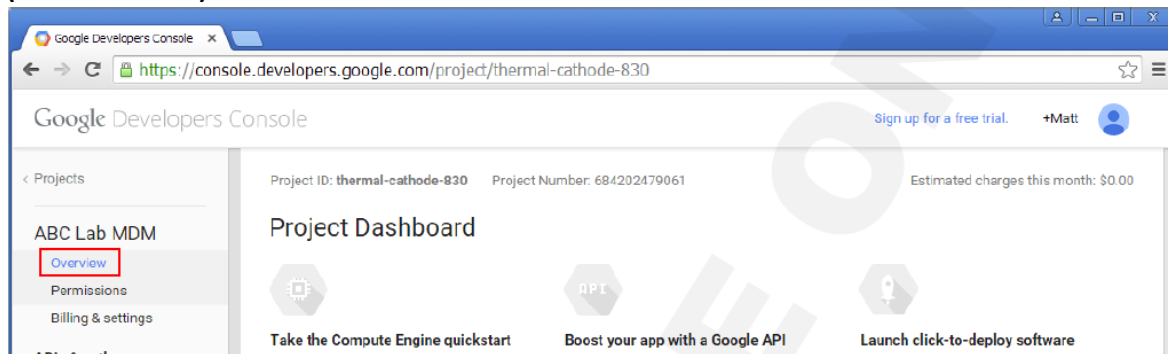
- k. Back on the Google Developers Console page that was left open, select and copy the value of the API key field



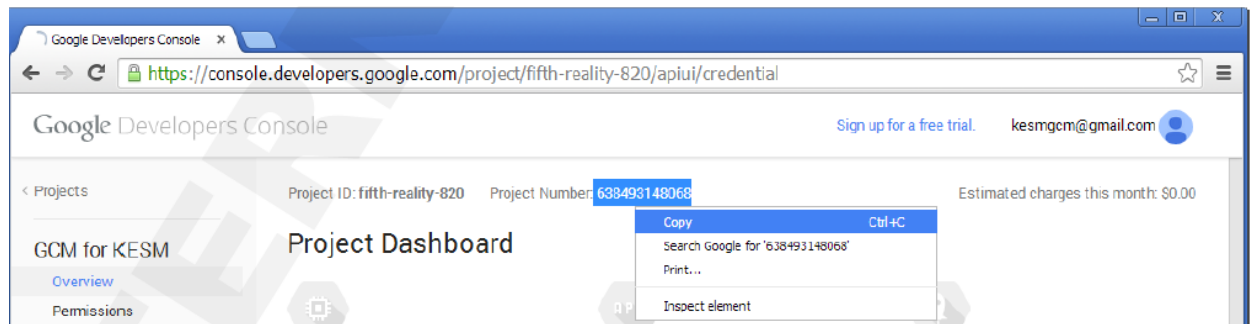
- I. Paste this into the API Key area in the Google Cloud Messaging Settings area (outlined in red)



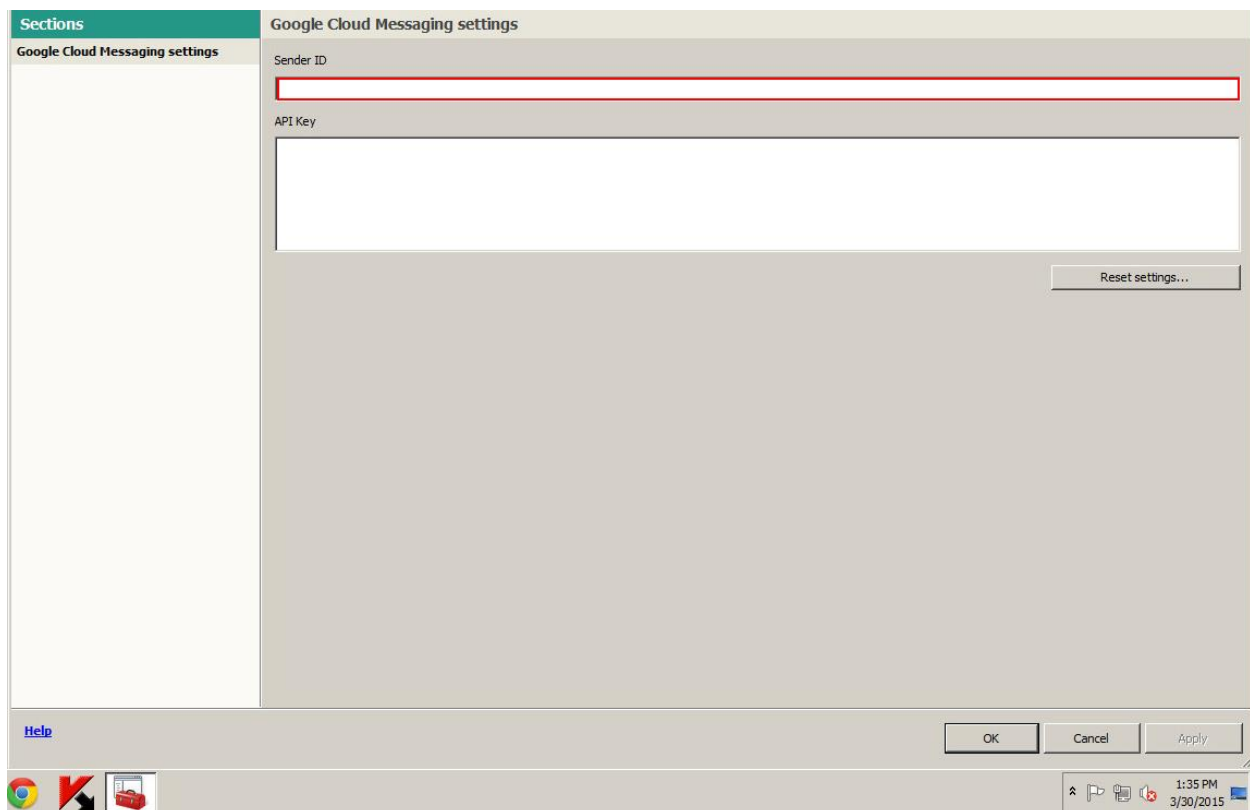
- m. Back on the Google Developers Console, select the Overview node in the left hand pane (Outlined in red)



n. In the center of the screen, highlight and copy the Project number



o. Back on the KSC Admin Console, right click and paste the Project number into the Sender ID field (outlined in red below)



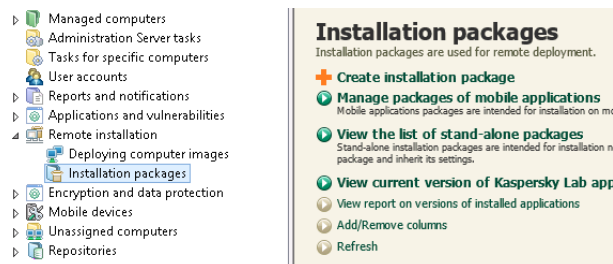
Click OK and then, reboot the KSC Admin Server.

IV. Install iOS Mobile Devices Server

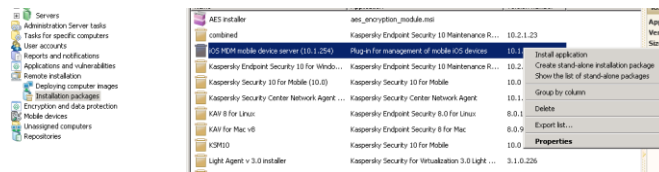
NOTE: this server component can be installed on the Security Center Administration Server, and another server/hardware platform is not required.

(Please see the appendix for illustrations of ports/connections needed)

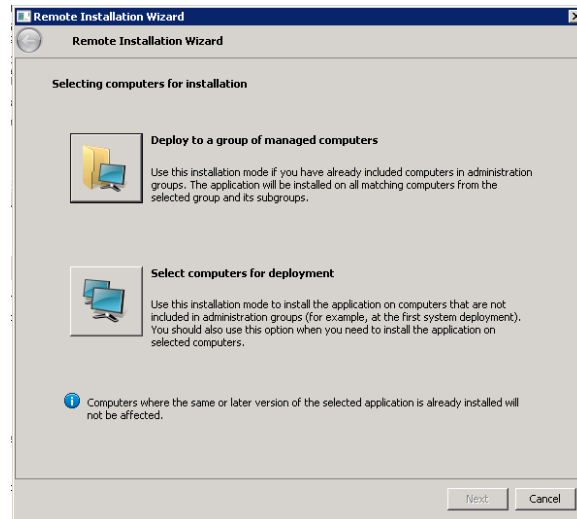
1. In the KSC window, expand the Remote Installation heading, and click on Installation packages below the heading:



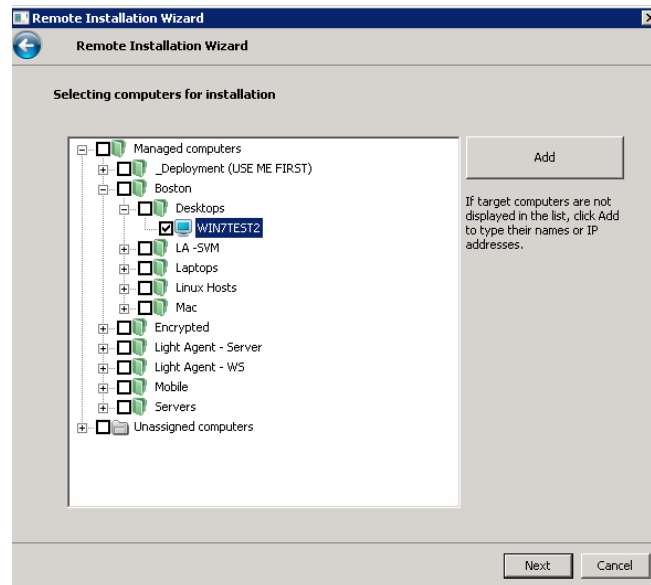
2. Right click on the iOS installation package and select Install Application:



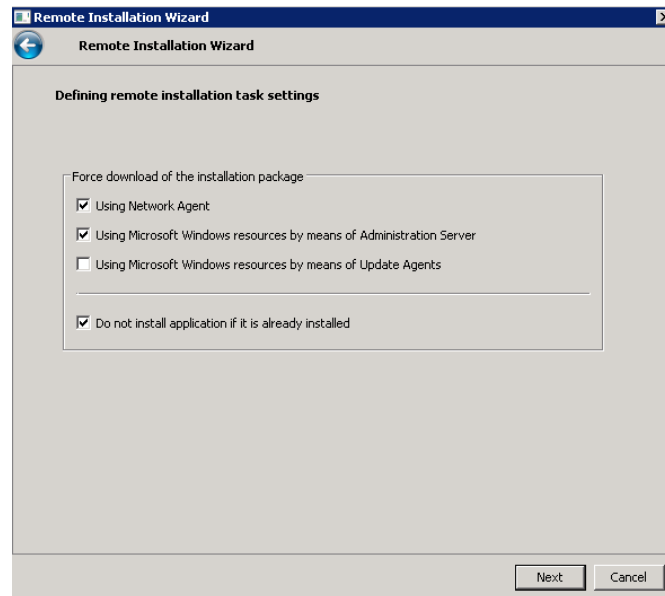
3. Click the button next to Select computers for deployment:



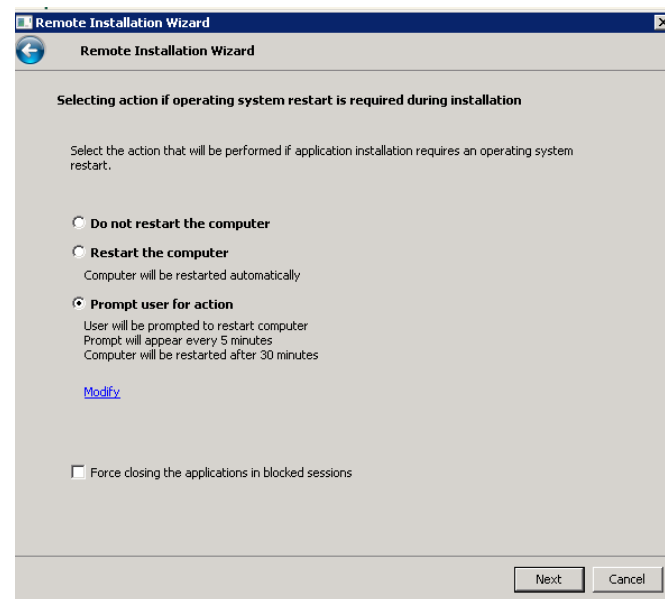
4. Click the plus sign next to Managed computers, and navigate to the machine where the iOS server software will be installed:



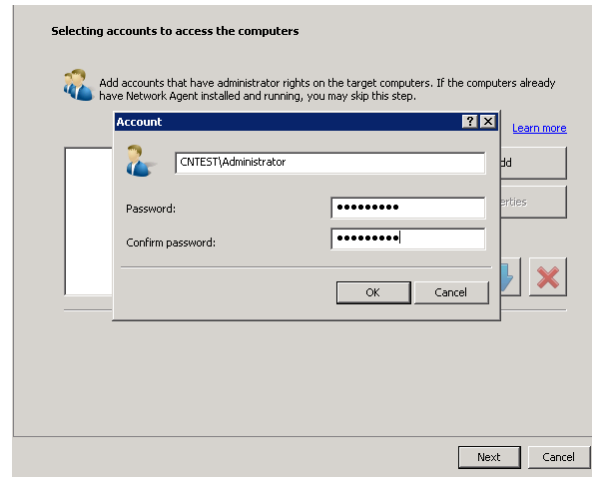
5. Click Next at the Defining remote installation task settings screen:



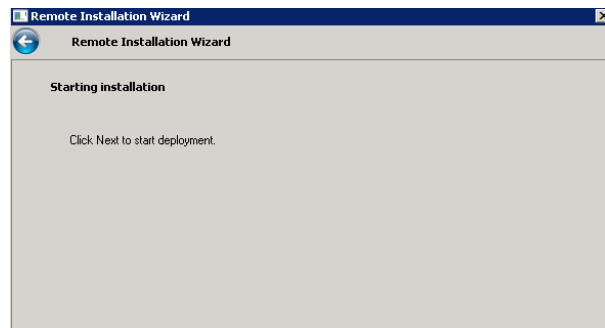
6. Click Next, selecting Prompt user for action if a restart is required:



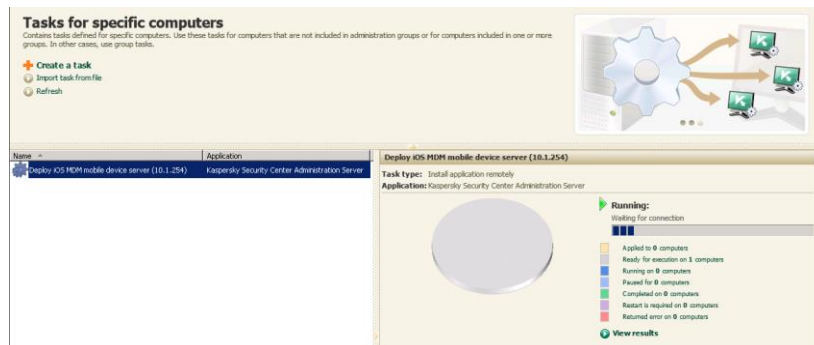
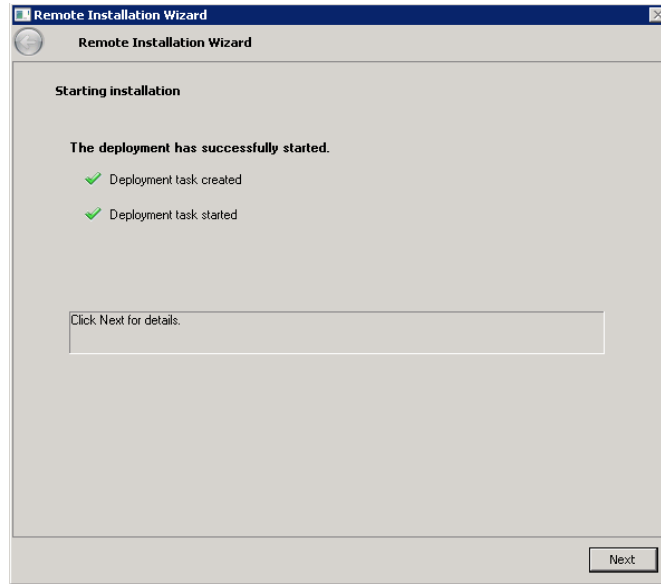
7. In the next screen, click Add to put in a domain administrator account to run the installation process. Click OK, then Next.



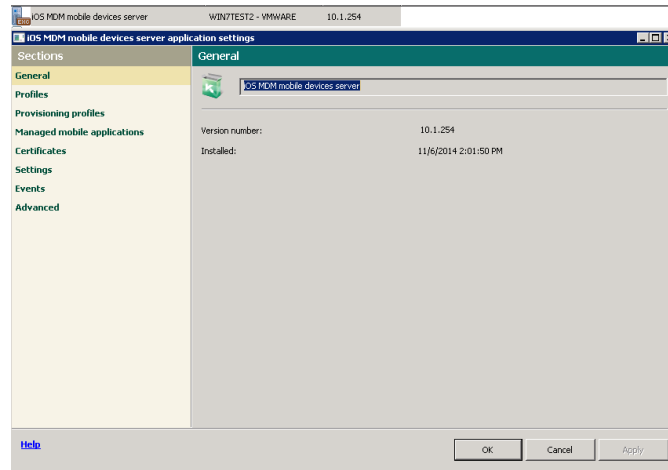
8. Click Next, as instructed here, to start deploying the iOS MDM server package



9. Click the Next button on the Starting Installation screen – you will then be redirected to the Tasks for specific computers:



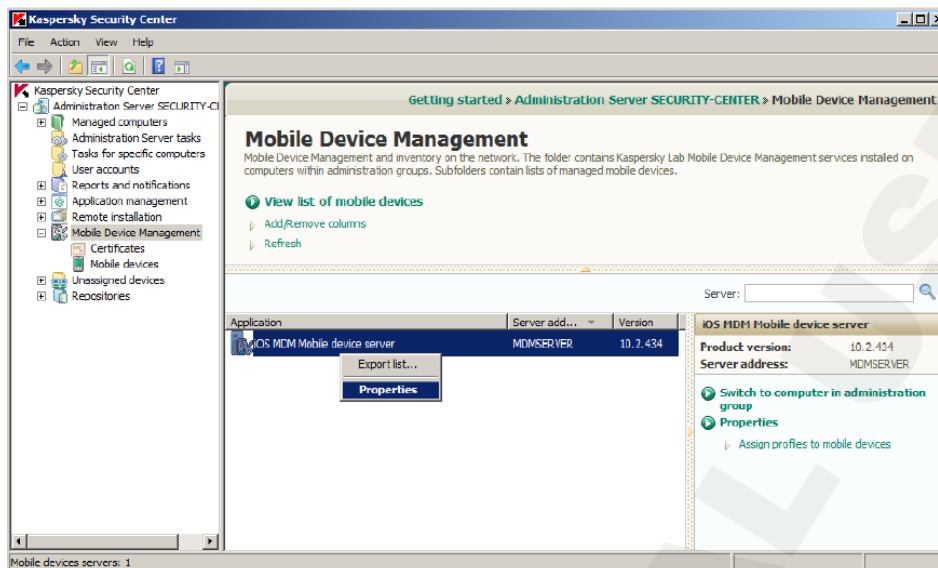
- Once the install is complete, the server will appear in the mobile devices server window Right click on the server and go to Properties



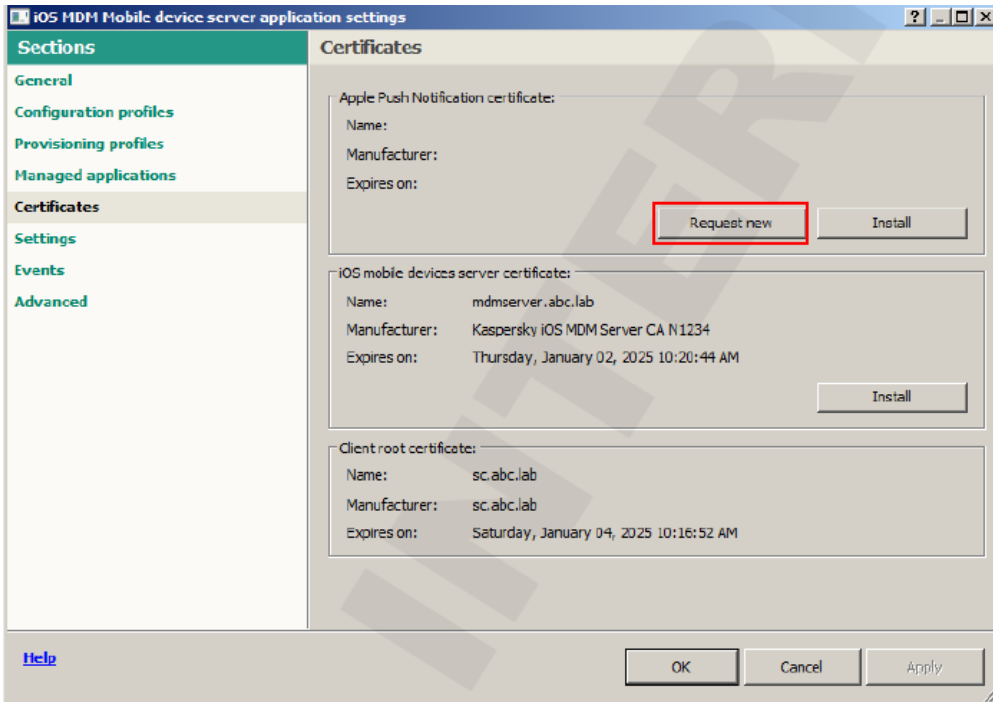
Create an APNs certificate

Connection to the Apple Push Notification service is needed to get connectivity to manage iOS devices remotely.

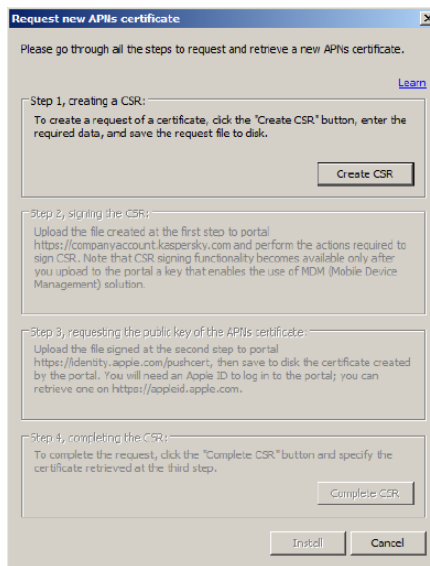
1. In the KSC Administration Server Console, click on the Mobile Device Management node in the left pane, and in the center pane, right click the iOS MDM Mobile device server and select Properties



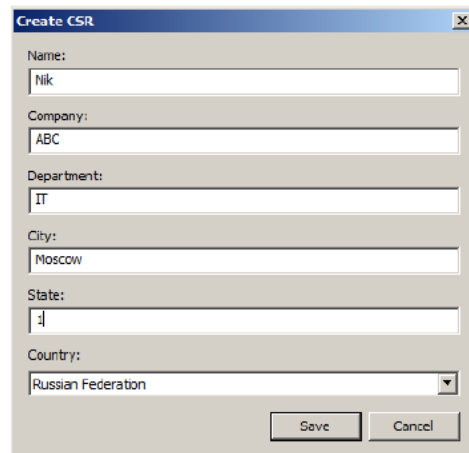
2. In the next screen, click on the Certificates node in the left hand pane, then in the right hand side of the screen, click the Request new button (outlined in red)



3. Click the Create CSR button:



4. In the next screen, fill in the form with as much data as you like, click Save:



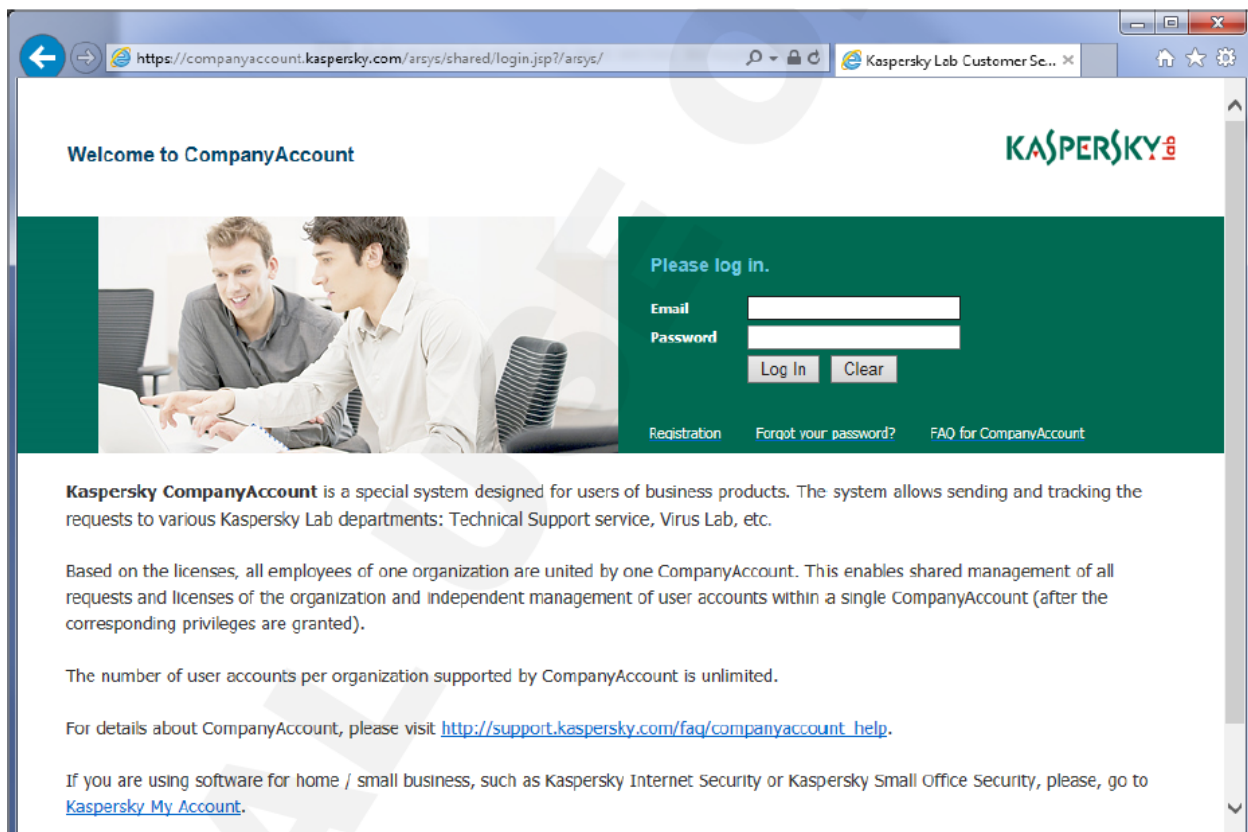
At the next dialog, name the file mycer,cer, for example, and save it to the computer.

5. **AT THE NEXT SCREEN, BE SURE TO KEEP THE SCREEN YOU SEE BELOW OPEN UNTIL YOU RECEIVE THE CERT FROM APPLE. IF YOU CLOSE THIS, YOU WILL HAVE TO START AGAIN!**

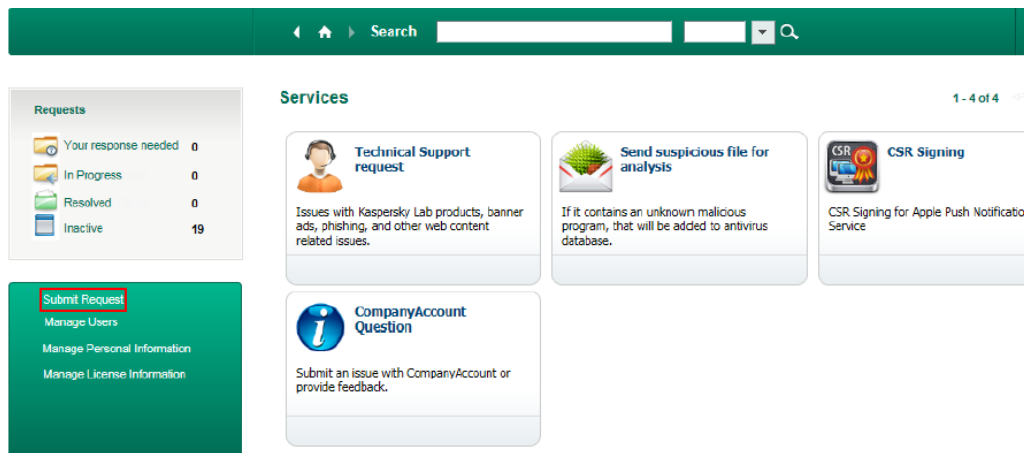


Signing a CSR – Step 1: Kaspersky Company.Account site

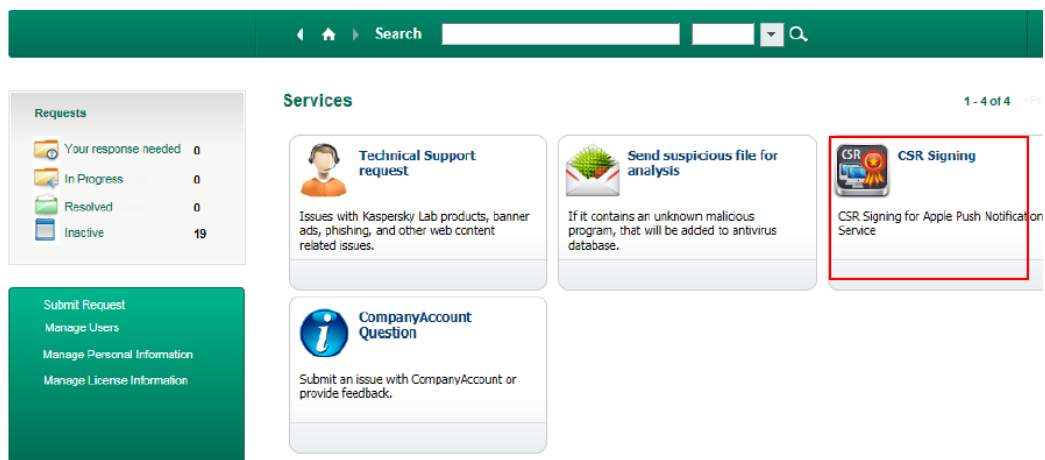
1. Sites need to create an account here – see <http://support.kaspersky.com/faq/companyaccount> help
2. In a browser, go to <https://companyaccount.kaspersky.com> (Be sure to allow the site to open popups)



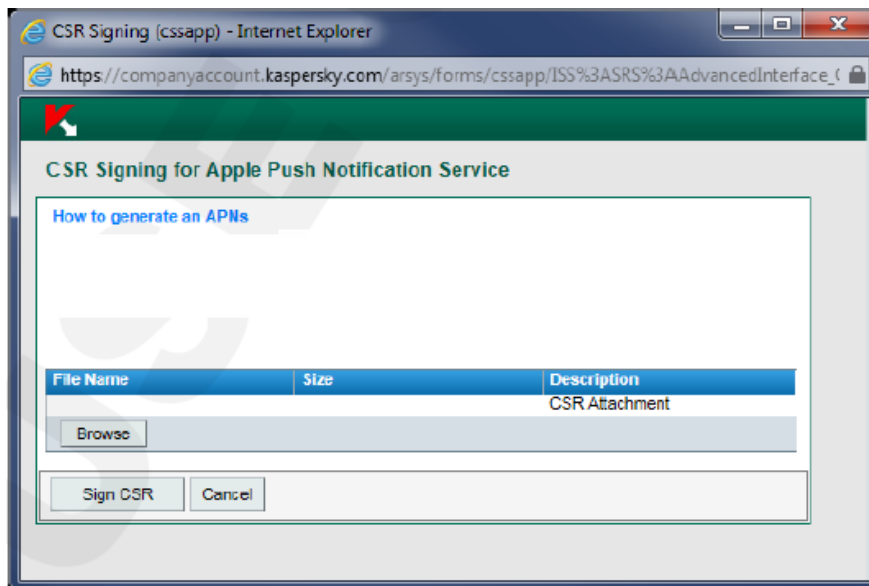
3. Log in to the site and at the next screen, click Submit Request (the first option in the green box to the left (outlined in red))



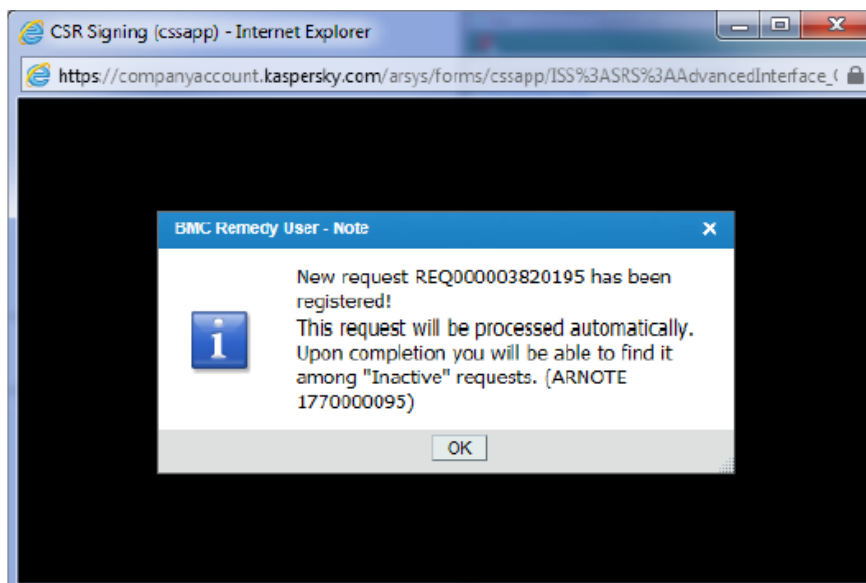
4. In that same page, click on CSR Signing to the upper right (also outlined in red)



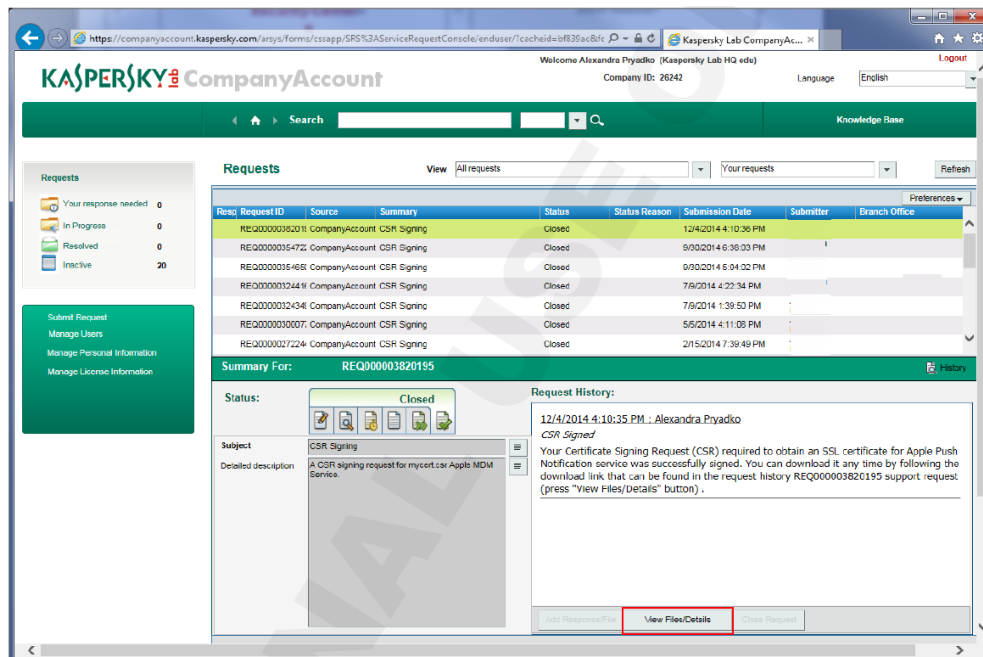
5. In the screen that opens, click on Browse, then Choose file, and select the myfile.csr we saved in the last step



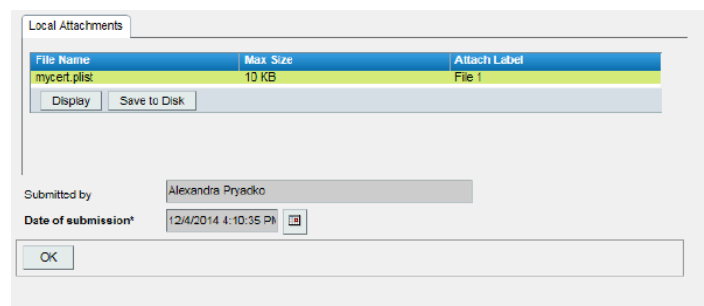
6. Click the Sign CSR button in that screen and in the next screen, click OK to close the message warning that the request will be processed automatically:



- After this, the list of request opens automatically. Click the latest one at the top of the list and click View Files/Details in the lower right (outlined in red, below)



- In the Local Attachments table, select the row with the mycert.plist file listed. When the two buttons appear below the line, click Save to Disk.



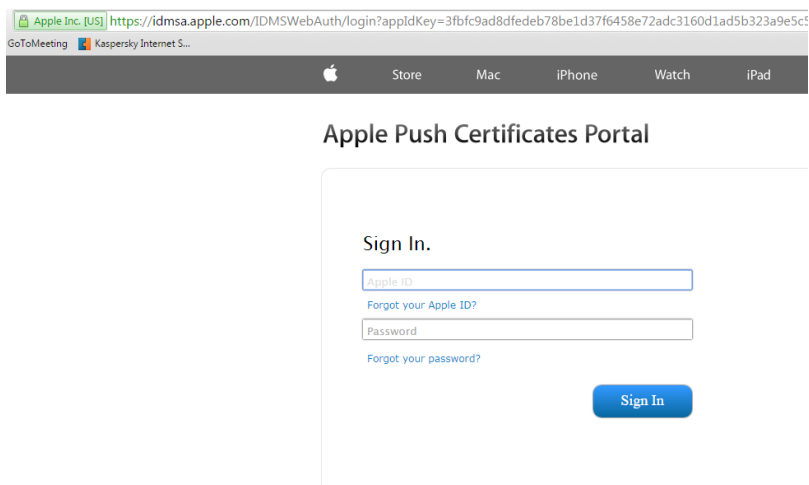
The file that is save is mycert.plist -

- Close the browser.

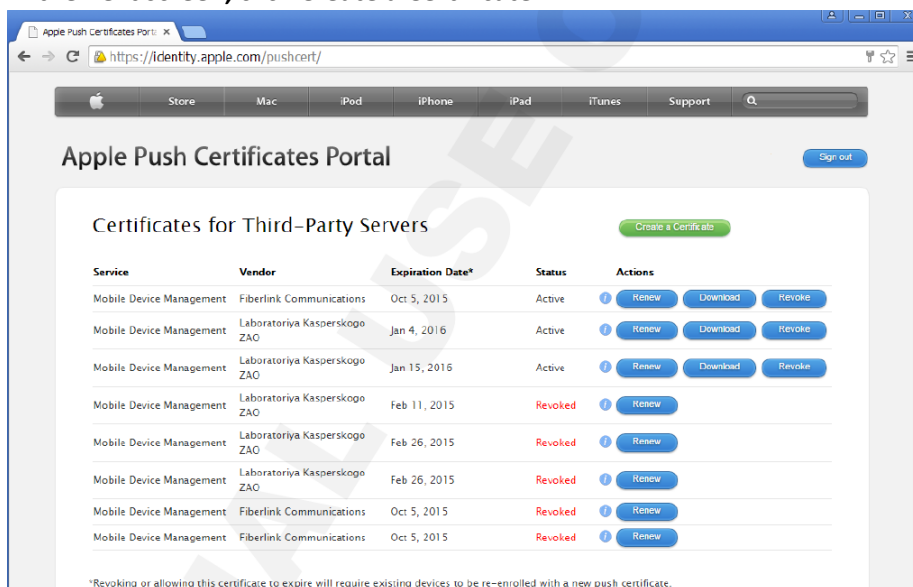
Signing a CSR – Step 2: apple.com

The next step in setting up the APNs connection is to get the plist file, created in the last step, to be signed at the Apple website.

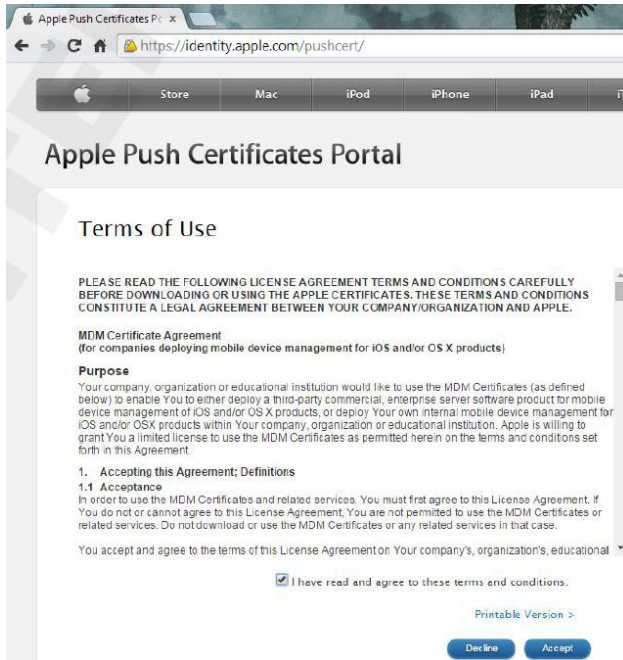
1. Go to <https://identity.apple.com/pushcert> and log in using your Apple id



2. In the next screen, click Create a Certificate



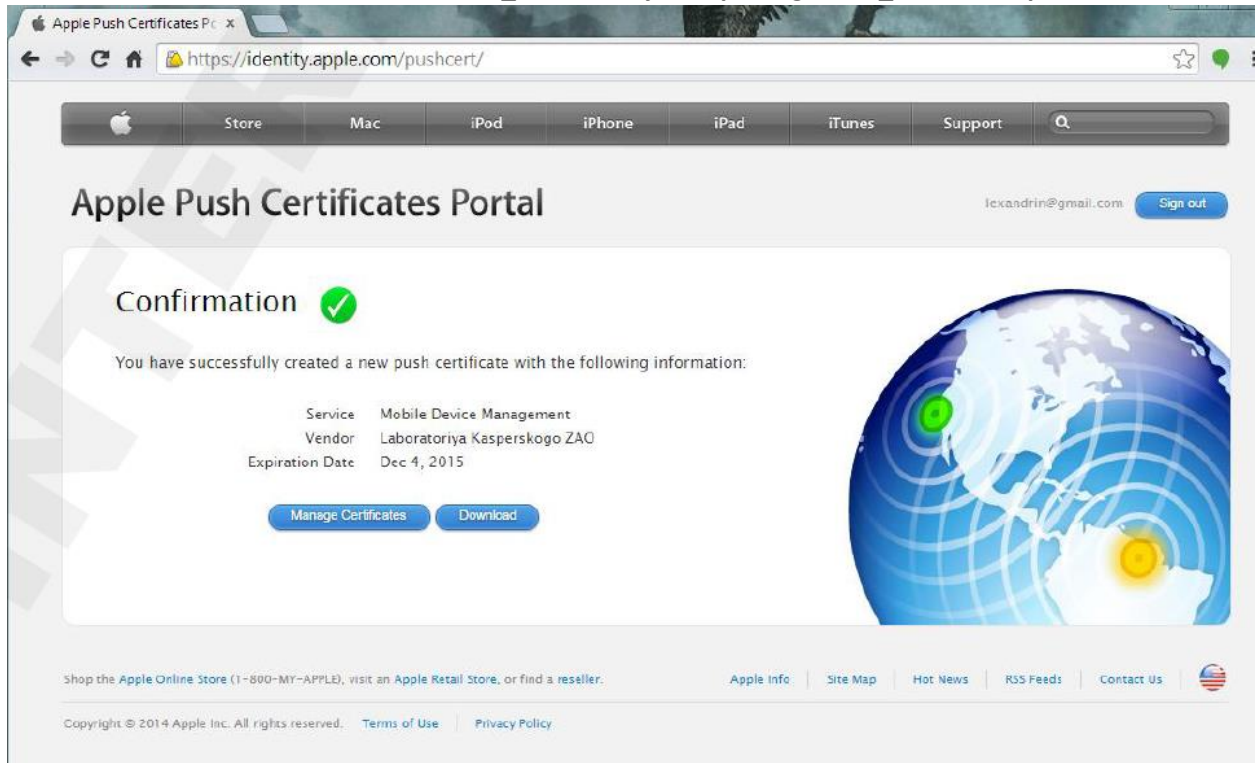
3. Then, click **Accept** in the Terms of Use screen lower right,



4. In the next screen, click on **Choose File** and select the mycert.plist created earlier, and click **Upload**:



- Next, click Download and save the MDM_Laboratoriya Kasperkogo ZAO_Certificate.pem file



- Close the browser you have to apple.com and copy the .pem file from the last step to the Security Center Server.

Installing the APNs certificate on the KSC

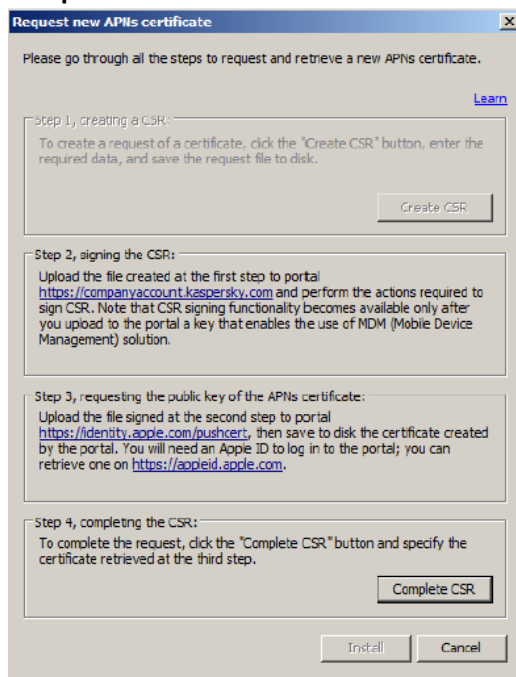
The .pem file needs to be loaded onto the Kaspersky Security Center (KSC) server, and when completed, a certificate with a .pfx extension is the result. This is the certificate to be installed on the iOS MDM server.

NOTE: if the iOS server is a separate platform, make certain that the port and address ranges needed for APNs are accessible from the KSC Server.

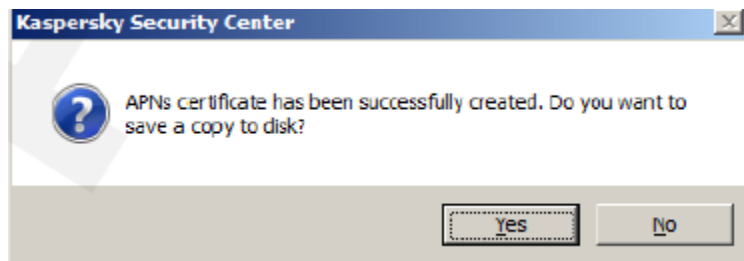
The IP Address range is 17.0.0.0/8 and must be accessible over ports 2195 and 2196.

When installing the iOS server, the communications are checked and if failing, an error is put in the installation log.

1. Return to the KSC Admin server, and the Request new APNs certificate dialog box should still be open:

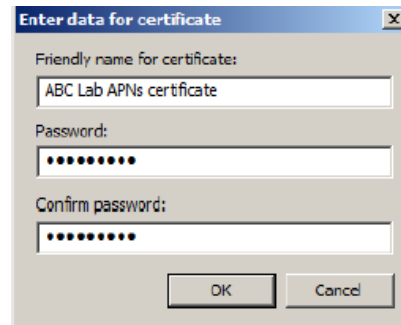


2. Click Complete CSR and select the MDM_Laboratoriya Kasperkogo ZAO_Certificate.pem from the previous steps and click Open
3. In the next dialog window, click Yes:

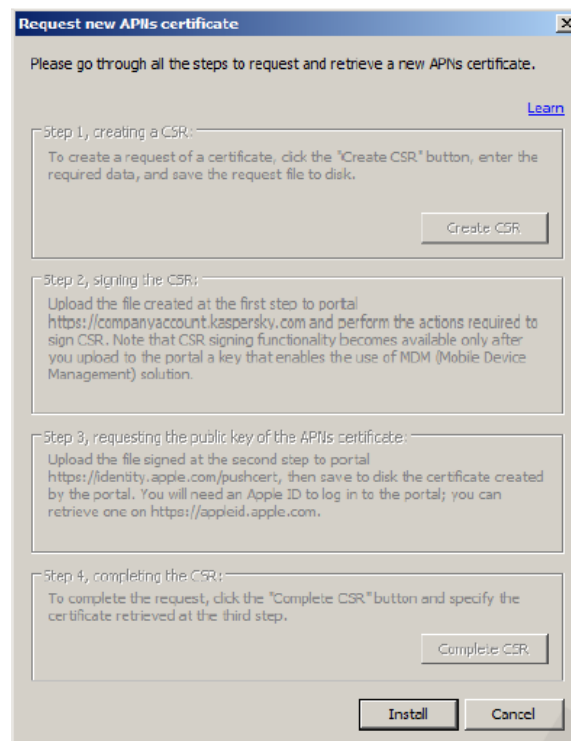


4. Type the name mycert and click OK

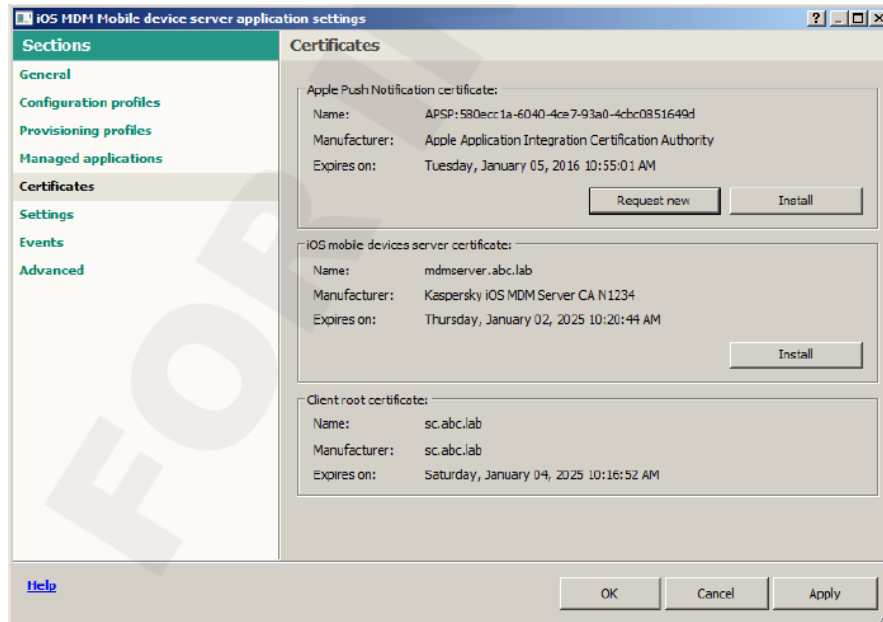
- In the next window, type a name (in this example, ABC MDM-server certificate, but make it specific to the install here) and a password and click OK:



- When the message appears that the certificate has been saved successfully, click OK.
- Click Install to complete the Request Wizard:



8. Check the Certificates screen, to confirm the certificate has been installed correctly:



9. Click OK to exit the iOS MDM Mobile Devices server properties window.

V. Install Self-Service Portal

The self-service portal is a new part of the Kaspersky tool kit for MDM. It allows authorized users to connect their mobile devices to the Kaspersky Security Center, and to install software management components.

Some functionality available on the Self Service portal:

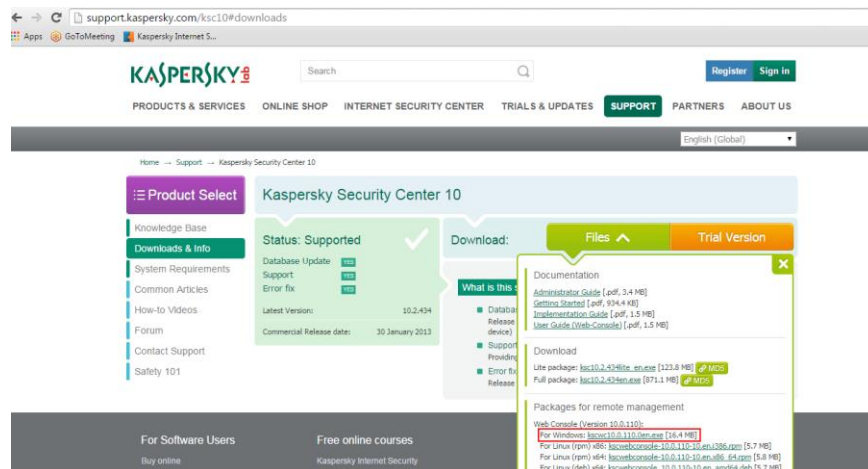
- Lock (Android and iOS)
- Unlock (Android and iOS)
- Locate (Android)
- Set off alarm (Android)
- Take a photo “the MugShot “ (Android)
- Wipe all or just corporate data (Android and iOS)

The Self-Service Portal (or SSP) can be installed on a separate Windows or Linux machine or VM, or can be installed on the KSC Administration Server.

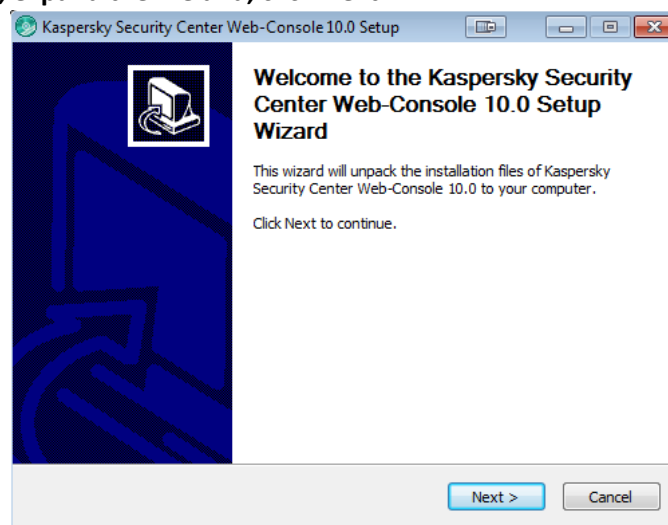
The following process outlines the installation onto the KSC Administration Server.

Also, please see the appendix for illustrations of ports/connections needed.

1. From the web page <http://support.kaspersky.com/ksc10#downloads>, click the Green block and download the kscwc10.0.110.0en.exe file (outlined in red below):

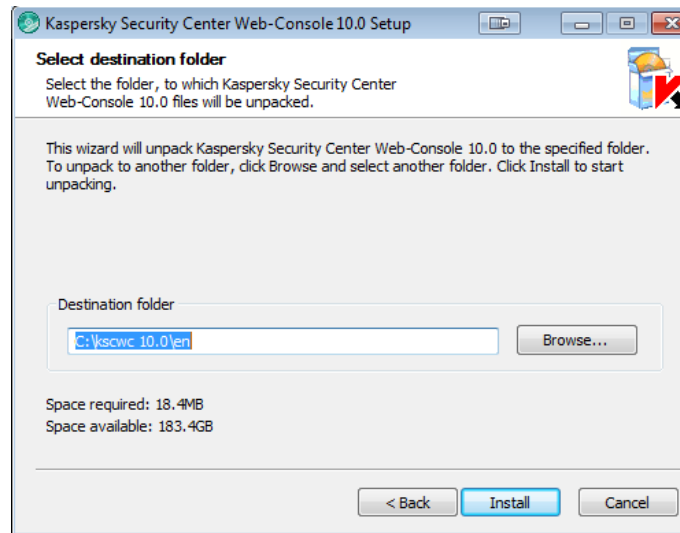


2. After downloading, expand the file and, click Next:

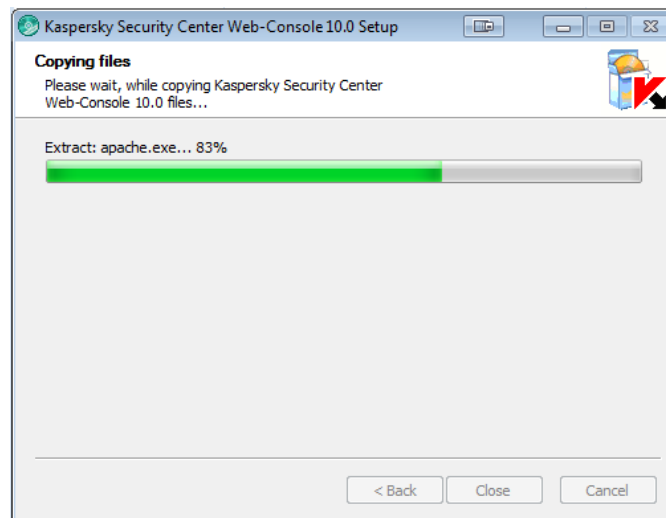


3. In the next screen, if needed, change the directory to expand the installer to, then click Install:

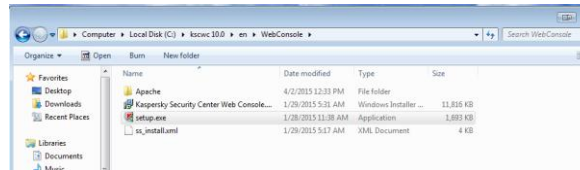
4.



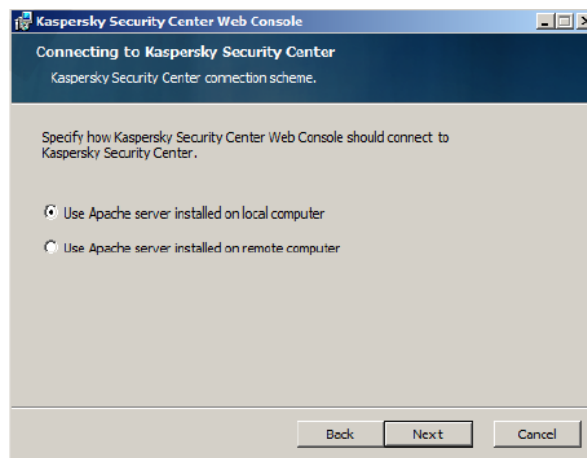
The expander continues:



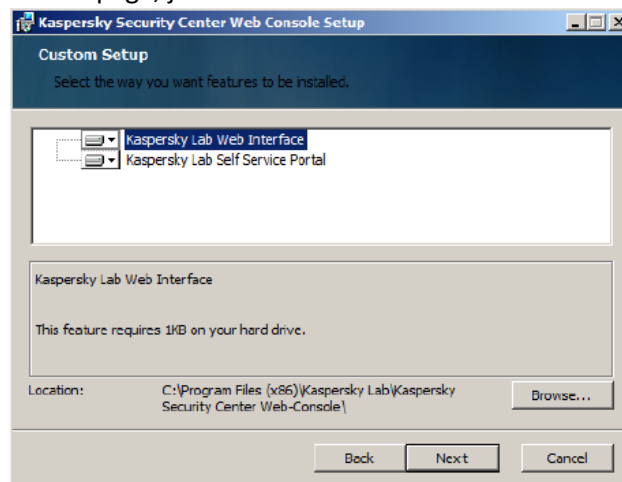
In the resulting folder, right click the setup.exe file and click on Run as Administrator



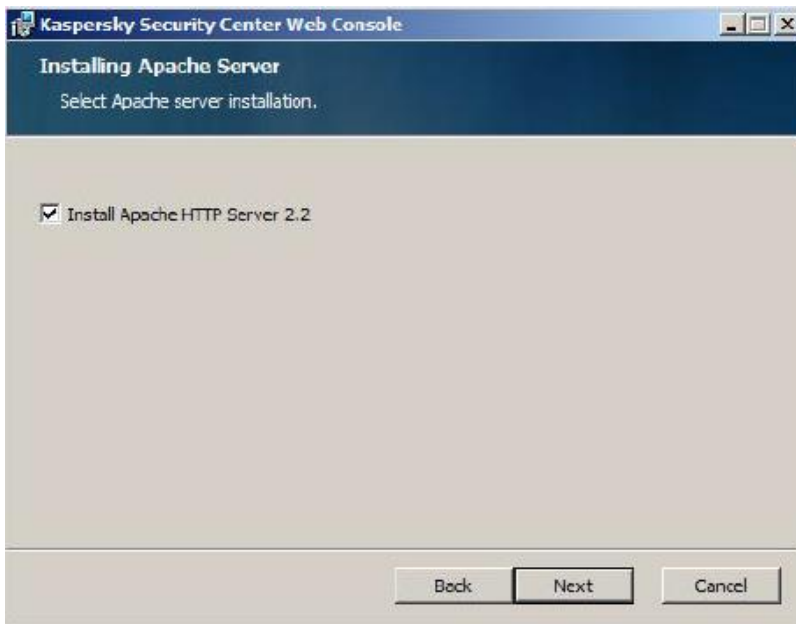
- On the welcome and license agreement pages, click Next.
- At the next window, click Use Apache server installed on local computer and click Next:



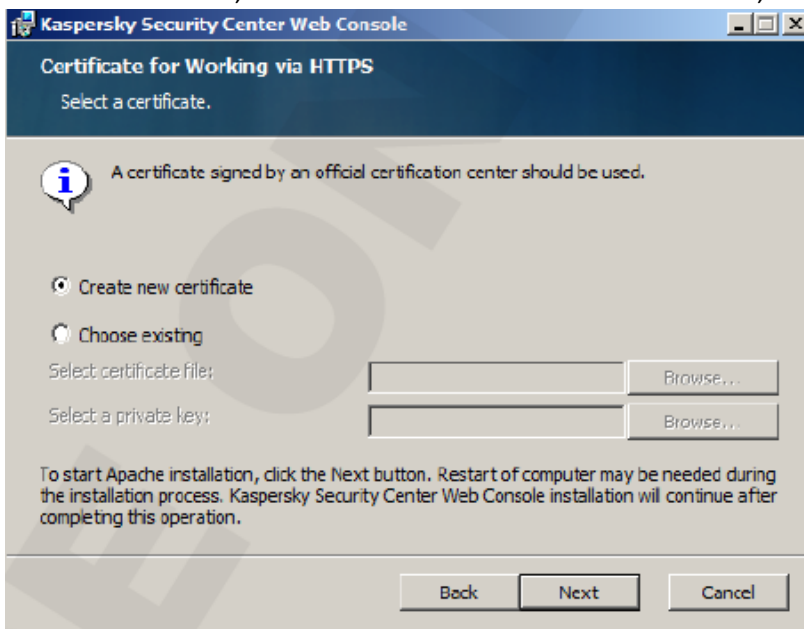
- On the Component selection page, just click Next and take the defaults:



- At the Installing Apache Server window, click Next as well:



- In the next window, make sure to select Create New Certificate, and click Next:



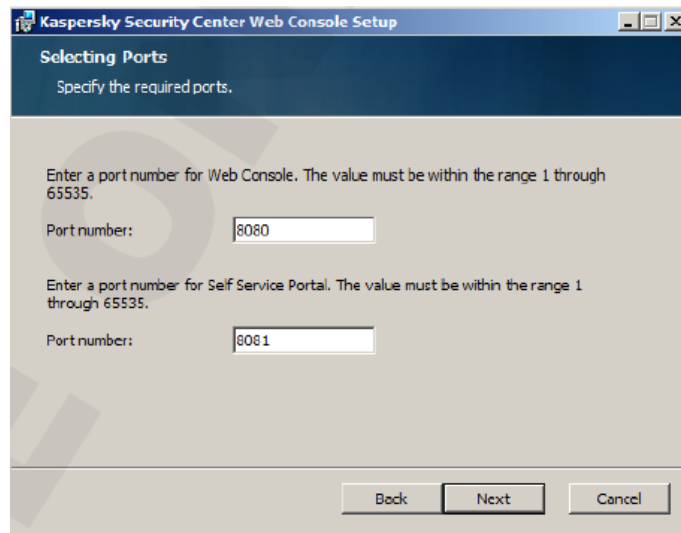
10. In the next window, type in the domain name, the external IP address of the machine and the Administrator's email address, as below, and click Next:

The screenshot shows a dialog box titled "Kaspersky Security Center Web Console" with the subtitle "Configuring the installation of Apache server". Below the subtitle, it says "Specify installation settings." There are three input fields: "Domain name:" with the value "abc.lab", "Server name:" with the value "192.168.2.100", and "Administrator's email address:" with the value "admin@abc.lab". At the bottom, there are three buttons: "Back", "Next", and "Cancel".

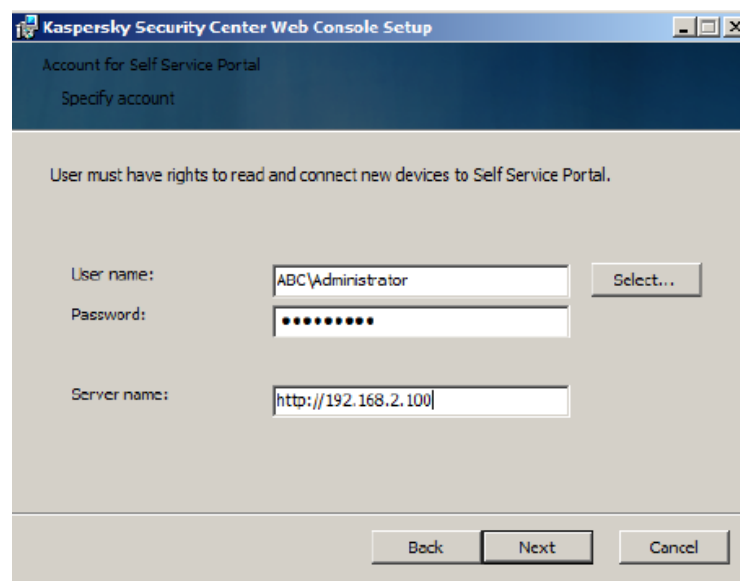
11. The next window contains the settings for connecting to the server – fill in the IP address of the Administration server, and keep the defaults, and click Next:

The screenshot shows a dialog box titled "Kaspersky Security Center Web Console" with the subtitle "Selecting Ports". Below the subtitle, it says "Specify the required ports." There are three input fields: "SSL port number:" with the value "13291", "Port number:" with the value "9000", and "Server address:" with the value "10.28.0.20". There is also a checkbox labeled "Connection gateway" which is unchecked. At the bottom, there are three buttons: "Back", "Next", and "Cancel".

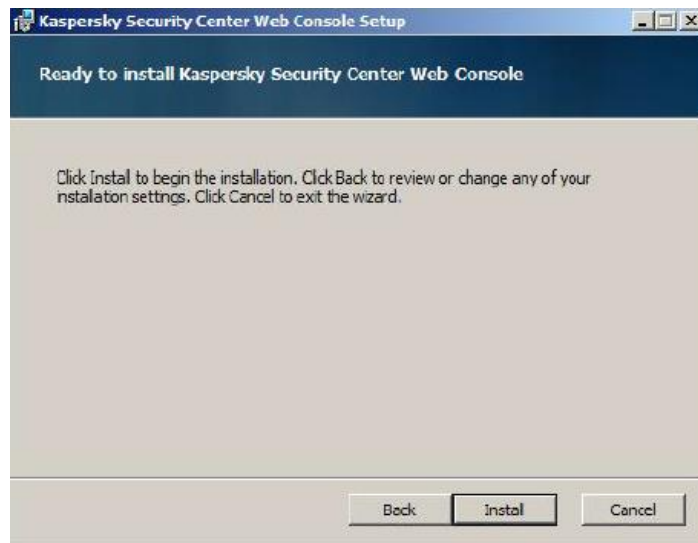
- The next window shows the ports to connect to the Web Console and the Self Service portal, Click Next to accept the defaults.



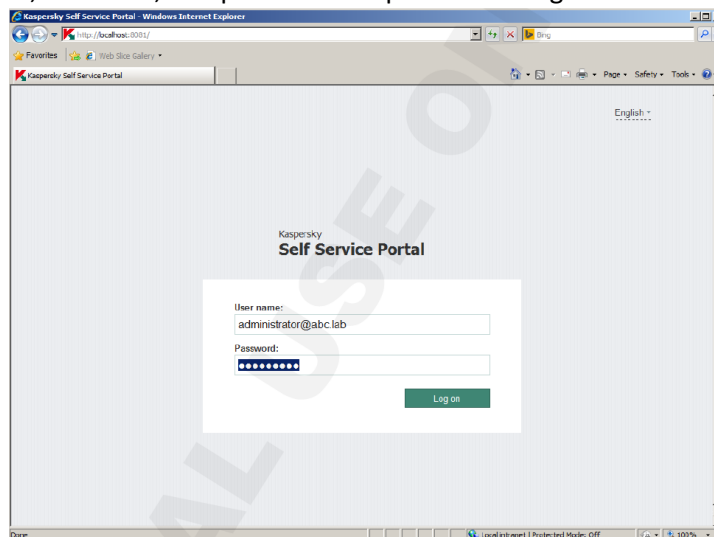
- ON the Account for Self Service Portal page, enter in the domain administrator account, and click Next, then enter the IP Address of the machine, starting with the http:// prefix, and click Next:



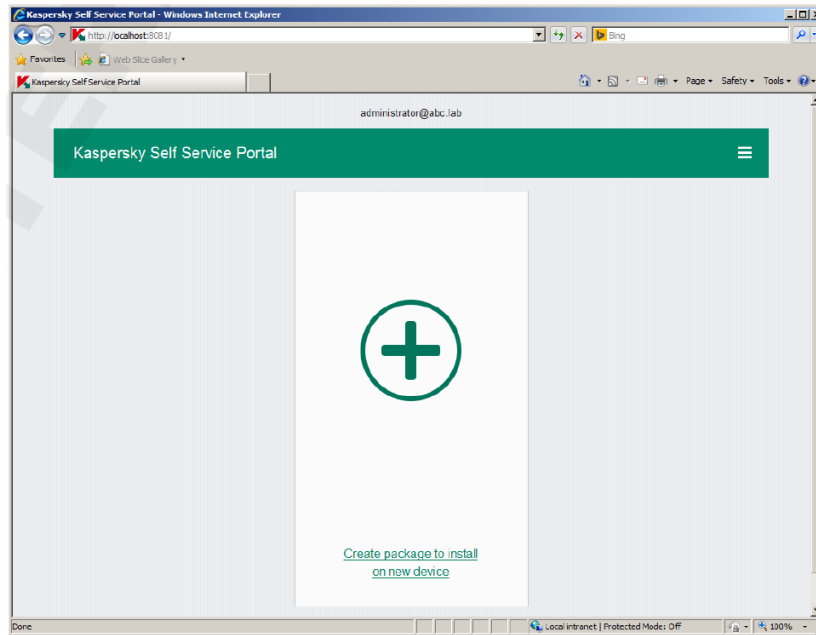
14. Click Install at the next window, and when complete, click Finish:



15. When this is complete, to test, open a browser on the server and go to <http://localhost:8081>. Accept the license agreement, and when presented with the login page, type in the administrator name, as shown, and password as specified during the installation:



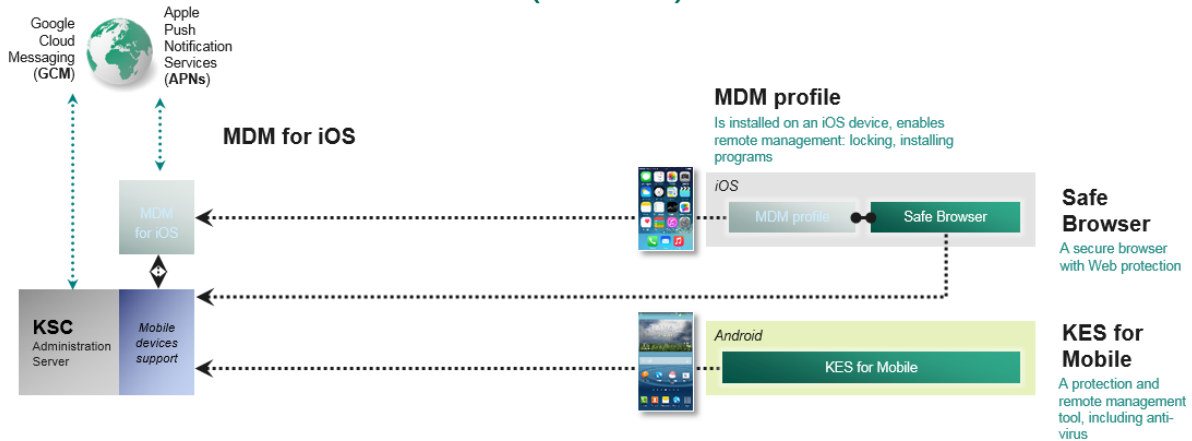
16. This is the logged in first page of the Self Service Portal.



Up to Pg 57 of kl010.10_sp1_en_labs.v6.3.2.pdf

Appendix: Connection Diagram with Port information

KASPERSKY ENDPOINT SECURITY FOR MOBILE (KESM)



ADMINISTRATION SERVER - CONNECTIONS

Ports on GCM (ASN 15169):

TCP 443



Connections with MDM server and Self-Service Portal:

- TCP 13000
- TCP 14000
- UDP 15000



Connections with mobile devices:

- TCP 13292
- TCP 17100

For downloading applications and MDM profiles from KSC webservice:

- TCP 8060
- TCP 8061

Administration Server must:

- Be accessible from MDM for iOS
- Be accessible from Self-Service Portal (SSP)
- Be accessible from mobile devices
- Have access to Google Cloud Messaging (GCM)

IOS MDM SERVER - CONNECTIONS

Ports on APNS (17.0.0.0/8):

TCP 2195
TCP 2196



Connections with mobile devices:

TCP 443

Port for Administration Server connection requests:

UDP 15000

iOS MDM Server must:

- Have access to the Administration Server
- Have access to Apple Push Notification Service (APNs)
- Be accessible from mobile iOS devices

Can be installed on KSC Administration Server

SELF-SERVICE PORTAL - CONNECTIONS

The Self-Service Portal must:

- Have access to the Administration Server
- Be accessible from mobile devices

Can be installed on KSC Administration Server



For accessing web interface, downloading applications and MDM profiles:

TCP 8081

IOS DEVICES - CONNECTIONS

iOS devices will connect to:

- MDM server
- Administration Server
- APNs
- Self-Service Portal (optional)





ANDROID DEVICES - CONNECTIONS

Android devices will connect to:

- KSC Administration Server
- GCM (TCP 5228—5230)
- Self-Service Portal (optional)



iOS MDM Management – Component Details

MDM profile 	Safe Browser 
<ul style="list-style-type: none"> — Device Locking — Data wipe — Settings: Wi-Fi, accounts, ... — Installing/uninstalling applications 	<ul style="list-style-type: none"> — Web protection — Jailbreak detection — Locating a lost or stolen device — Restricting access to corporate data — Wiping corporate data