### 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:

Kaspersky Security Center Administration Server 🛛 💻 🗙
Custom Setup
Select the application reactives you want installed.
P      Access Control     Kaspersky Lab Cisco NAC Posture Validation Server     Mobile devices support
Administration Server manages Kaspersky Lab applications. An instance of Microsoft SQL Server is required to run this component. This component requires 63.4 MB free space on the hard disk.
Location: C:\Program Files (x86))Kaspersky Lab\Kaspersky Security Center\
Cancel     Cancel     Cancel

Page 1 | 47

Select network size, click Next:



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

Kaspersky Security	Center Administration Server 🛛 🗕 🗖 🗙
Account Select the user account to s	tart the Administration Server service.
Assign an account to start A administrator permissions to	dministration Server service. The account must have edit the Administration Server database.
KL-AK-81345E0F67211C	
C User account	
Account:	Select
Password:	
Confirm password:	
—© 2013 Kaspersky Lab ZAO. All I	Rights Reserved.
	< Back Next > Cancel

Kaspersky Security Center Administration Server
Database server
Select database server type.
Select the type of database server to which you want to connect Administration
Microsoft SOL Service
O 13 Karperdy (ab 700 0) Bights Received
< Back Next > Cancel

Kaspersky Security Center Administration Server	<b>– – ×</b>
Connection settings	
Specify Microsoft SQL Server parameters.	
Select the computer that hosts SQL Server.	
<ul> <li>Install Microsoft SQL Server 2008 R2 Express SP2 (Recommended)</li> </ul>	
C Choose existing	
SQL Server name:	Select
Database name: KAV	
-© 2013 Kaspersky Lab ZAO, All Rights Reserved,	
< Back Next >	Cancel

Page 3 | 47

Kaspersky Security (	Center Admini:	stration Server	<b>– –</b> X	
SQL Authentication Mod	e			
Choose Authentication Mode				
Choose the authentication m you select SQL Server Authe	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 Auther	entication Mode			
C SQL Server Authenticatio	n Mode			
Account:				
Password:				
Confirm password:	,			
	induts Reserved			
Check connection	< Back	Next >	Cancel	
Kaspersky Security	Center Admini	stration Server	- 🗆 X	
Shared folder				
Create a new shared folder	or select an existing	one.		
Shared folders store installa applications. Create a new s	tion packages and u shared folder or sele	pdates for Kaspersky La ct an existing one.	ъ	
Create a shared folder				
Folder:				
C:\Program Files (x86	i)\Kaspersky Lab\Ka	spersky Security Center	Select	
Shar	ed folder name: KL	SHARE		
C Select existing chared f	older			
\\CNSERVER2012\cap	oluci	Ŧ	Select	
–© 2013 Kaspersky Lab ZAO. All F	Rights Reserved.			
	< Back	Next >	Cancel	
Kaspersky Security	Center Admini	stration Server	- 🗆 X	
Connection settings	derrear rearran			
Specify settings to connect to Administration Server.				
		teris destantiles		
Enter the Administration Server ports. Port numbers must be within the range of 1 to 65535.				
Bort pumber:	14000			
col	11000			
SSL port number:	13000			
@ 2012 Kame	© 2013 Kasperdy Leb 700 All Pichts Reserved			
G 2013 Kaspersky Lab ZAO, All F	< Back	Next >	Cancel	

Page 4 | 47

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

Kaspersky Security Center Administration Server 📃 🗖 🗙			
Administration Server address			
Specify Administration Server address.			
Set the Administration Server address to one of the following options:			
<ul> <li>DNS name. Used if a DNS server is present and client computers can get the address of Administration Server from it.</li> </ul>			
b. NetBIOS name. Used if client computers can get the address of Administration Server via the NetBIOS protocol, or if a WINS server is present in the network.			
c. IP address. Used only if the Administration Server has a static IP address which will not be changed in the future.			
Administration Server address:			
192.168.8.21			
—© 2013 Kaspersky Lab ZAO. All Rights Reserved. ————————————————————————————————————			
< Back Next > Cancel			

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

Kaspersky Security Center Administration Server			
Administration Server Address for Mobile Devices Connection Specify Administration Server address for mobile devices connection.			
Provide address that mobile devices will use to connect to the Administration Server.			
Be careful, SSL handshake may fail in case of address mismatch.			
Administration Server address for mobile devices connection:			
192.168.8.21			
—© 2013 Kaspersky Lab ZAO. All Rights Reserved.			
< Back Next > Cancel			

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)

Kaspersky Security Center Administration Server	x		
Plug-ins			
Select plug-ins to be installed.			
List of plug-ins:			
Kaspersky Endpoint Security 10 Maintenance Release 1 for Windows Console Plug-ir     Kaspersky Endpoint Security 10 for Windows Console Plug-in     Kaspersky Endpoint Security 8 for Mac Console Plug-in     Kaspersky Endpoint Security 8 for Windows Console Plug-in     Kaspersky Endpoint Security 8.0 for Linux Console Plug-in     Kaspersky Endpoint Security 8.0 for Linux Console Plug-in			
Kaspersky Security for Virtualization 2.0      Plug-in for Exchange ActiveSync      Plug-in for Novel      Plug-in for management of mobile IOS devices      V			
-© 2013 Kaspersky Lab ZAO. All Rights Reserved.			

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)

Sections	Settings	
Seneral Svents Keys	Administration Server connection settings           If you change a port number, the connection will be closed and you will need to reconnect to the Server.	
CSN proxy server Settings /irus outbreak Fraffic Events storage	Port number:     14000     integrad       SSL port number:     13000     integrad       SSL port for the Administration Console:     13291     integrad       SSL port for activation proxy server:     17000     integrad	
leb server ecurity Iser roles dvanced	✓ Open port for mobile devices         Port for mobile devices:         13292         Port to activate mobile clients:         I7100         Administration Server certificate	
	<ul> <li>Automatically assign computers the Update Agent status</li> <li>Administration Server can select Update Agents automatically. Clear the checkbox if you want to select Update Agents manually.</li> </ul>	

Page 6 | 47



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:

Sections	Web server
Sections General Events Keys KSII proxy server Settings Virus outbreak Traffic Events storage Web server Security User roles Advanced	Web server         Kaspersky Security Center web server is designed for storing and transmitting stand-alone installation packages and mobile device profiles over the network.         Learn more.u.         Administration Server connection settings         Over HTTP:         Web Server domain name:         Web Server HTTP port:         0ver HTTPS:         Web server HTTPS port:         @ Specify certificate through Administration Server tools         C Specify another certificate
ttelp	OK         Cancel         Apply           * [P 10]         121 PM           3/30/2015         =

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 clien	t management
5229	outbound	android.apis.google.com	for clien	t management
5230	outbound	android.apis.google.com	for clien	t 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

S Google Developers Console ×	
← → C 🖀 https://accounts.google.com/ServiceLogin?service=cloudconsol	2&passive=true&continue=https%3A%2F%2Fconsole.dev ☆ 📄 🚍
Google	Í
One account. All	of Google.
Sign in to continue to Google De	evelopers Console
Email Password Sign in ✓ Stay signed in Create an account One Google Account for every M M M III № III №	Need Help?

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

Page 9 | 47

Google Developers Console X	
← → C 🖀 https://console.developers.google.com/project	☆] ≡
Google Developers Console	Sign up for a free trial. kesmgcm@gmail.com
Projects Baling Account settings Naed help? Privacy & terms (3	Projects are used to group resources. To get started, create your first project.
~~	

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

	ie.developers.googie.com/project			23
			ior a free trial. +N	latt
			1	
	New Project			
ccount settings	PROJECT NAME			
	ABC Lab MDM			
	PROJECT ID			
	thermal-cathode-830	C		
	I have read and agree to all Terms of Service for the Google Cloud Platform products.			
	Create Cancel			
			1	

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

Google Developers Console 🗙		
← → C 🔒 https://cor	nsole.developers.google.com/project/thermal-cathode-830	≣ [کړ
Google Developers	s Console	Sign up for a free trial. +Matt
< Projects	Enabled APIs Some APIs are enabled automatically. You can disable them if y	you're not using their services.
ABC Lab MDM	NAME A	QUDTA STATUS
Permissions Billing & settings	BigQuery API	0% ON
ADIe & outh	Debuglet Controller API	0% ON
APIs	Gcogle Cloud SQL	ON
Credentials Consent screen	Google Cloud Storage	ON
Push	Google Cloud Storage JSON API	ON
Monitoring		
Source Code	Browse APIs	
Compute Networking	Filter by API name or description	
Storage	NAME ^	QUDTA STATUS
Big Data	Ad Exchange Buyer API	1,000 requests/day OFF
Cunnort	Ad Exchange Seller API	10,000 requests/day OFF

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

→ C  https://co	nsole.developers.google.com/project/thermal-cathode-830/apiui/api			ŝ
Google Developer	s Console	ign up for a free trial.	+Matt	
rojects	Enabled APIs Some APIs are enabled automatically. You can disable them if you're not using their services.			
BC Lab MDM	NAME A	QUOTA		STATUS
Permissions	BigQuery API		0%	ON
Pls & auth	Debuglet Controller API		0%	ON
APIs	Google Cloud SQL			ON
Credentials Consent screen	Google Cloud Storage			ON
Push	Google Cloud Storage JSON API			ON
ource Code ompute	Browse APIs			
etworking	Cloud Messaging for Android ×			
orage g Data	NAME A	QUOTA	A	STATUS
9	Google Cloud Messaging for Android Google Cloud Messaging allows for push messaging to And	roid devices. none		OFF

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

Google Developers Console			A - B X
← → C 🖀 https://cons	ole.developers.google.com/project/thermal-cathode-830/apiui/api		☆ =
			+Matt
	Enabled APIs		
ABC Lab MDM	Some A Enable the Google Cloud Messaging for Android		
Overview Permissions Billing & settings	BigCure Cloud Messaging for Android Terms of Service and Google Cloud Messaging for Android Terms of Service.		0% ON
APIs & auth	Debuon Accept Cancel		0% ON
APIs Credentials Consent screen	Google Boogle Cloud Storage		0N ON
Push Monitoring	Boogle Cloud Storage JSON API-		ON
Source Code Compute	Browse APIs		
Networking	Cloud Messaging for Android 🛛 🔀		
Storage Big Data			
	Boogle Cloud Messaging for Android Google Cloud Messaging allows for push messaging to And	roid devices. none	OFF

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

← → C 🖀 https://console.developers.google.com/project/thermal-cathode-830/apiui/api					
Google Developers Co	onsole	Sign up for a free trial.	+Matt		
ABC Lab MDM Overview Permissions	Enabled APIs Some APIs are enabled automatically. You can disable them if you're not using their services. NAME ^ BioCherry API	αυοτά	STATUS		
Billing & settings APIs & auth	Debugiet Controller API		-0% ON		
APIs Credentials Consent screen	Google Cloud Messaging for Android Google Cloud SQL		ON		
Push Monitoring Source Code	Google Cloud Storage Google Cloud Storage JSCN API		0N 0N		
Compute Networking Storage	Browse APIs Cloud Messaging for Android ×				
Support	No results found				



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:



Coogle Developers costs
C in https://console.developers.google.com/project/thermai-cathode-830/apiui/credential
C in the second in each result in the second in each result in the second in each result is usering parameter, if specified. If the usering parameter is in sisting, your machines in Padiess will be user in parameter in each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is usering parameter.google.com or each result is in the second in each result is in the second is in the second in each result i

#### 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.

Google Developers Console X				
← → C 🔒 https://consol	e.developers.google.com/projec	ct/fifth-reality-820/ap	iui/credential#	☆ =
Google Developers C	onsole		Sign up for a f	ree trial. kesmgcm@gmail.com
< Projects	specific data with you (for example, contact lists) while keeping their usernames, passwords, and other			
GCM for KESM	information private.			
Overview	Learn more			
Permissions				
Billing & settings	Create new Client ID			
APIs & auth				
APIS				
Credentials	Public API access	Key for server application	ons	
Consent screen	Use of this key does not require			
Push	any user action or consent, does	APTKEY	AlzaSyD-NhT8ztXsz4amjdZkwzi	ZbkXb0PITGz0s
Monitoring	not grant access to any account information, and is not used for	IPS	Any IP allowed	
Source Code	authorization.			
Compute	Learn more	ACTIVATION DATE	Jan 9, 2015, 4:55:00 AM	
Networking		ACTIVATED BY	kesmgcm@gmail.com (you)	
Storage	Create new Key			
Big Data		Edit allowed IPs	Regenerate key Delete	
Support				
~~				

#### 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:

Sections	Google Cloud Messaging settings
Google Cloud Messaging settings	Sender ID
	API Key
	Reset settings
Help	OK Cancel Accly
	▲ D> D= 0 1135PM
😕 🍢 🚳	* 🕞 🗐 🔞 3/30/2015 💻

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)

Sections	Google Cloud Messaging settings
Google Cloud Messaging settings	Sender ID
	APIKey
	Develophing
	Keset seturigs
нер	OK Cancel Apply
e 🔽 🛄	1:35 PM
🥑 🍢 🕍	* 🗗 🐜 3/30/2015 🂻

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)

Sections	Google Cloud Messaging settings
Google Cloud Messaging settings	Sender ID
	APIKey
	Reset settings
Help	
ICIP	OK Cancel Apply
o K 🗟	* 🕞 寣 🗘 1:35 PM

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:

Administration Server tasks     Administration Server tasks     Tasks for specific computers	AES installer	aes_encryption_module.msi Kaspersky Endpoint Security 10 Maintenance R	10.2.1.23	Applic
Reports and notifications	iOS MDM mobile device server (10.1.254)	Plug-in for management of mobile IOS devices	10.1. Install application	1 Janes
Applications and vulnerabilities	Kaspersky Endpoint Security 10 for Windo	Kaspersky Endpoint Security 10 Maintenance R	10.2. Create stand-alone installation p	ackage
Remote installation Deploying computer images	Kaspersky Security 10 for Mobile (10.0)	Kaspersky Security 10 for Mobile	10.0 Show the list of stand-arone pace	tages
📑 Installation packages	Kaspersky Security Center Network Agent	Kaspersky Security Center Network Agent	10.1. Group by column	•
Encryption and data protection Mobile devices	KAV 8 for Linux	Kaspersky Endpoint Security 8.0 for Linux	8.0.1 Delete	
Unassigned computers	KAV for Mac v8	Kaspersky Endpoint Security 8 for Mac	8.0.9 Export list	
Repositories	KSM10	Kaspersky Security 10 for Mobile	10.0 Properties	
	Light Agent v 3.0 installer	Kaspersky Security for Virtualization 3.0 Light	3.1.0.226	

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:

Remote Installation Wizard	×
G Remote Installation Wizard	
Selecting computers for installation	
	Add If target computers are not displayed in the list, click Add to type their names or IP addresses.
	Next Cancel

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

Remote Installation Wizard	I		
Defining remote installation ta	sk settings		
Force download of the installation	n package		
Using Network Agent			
Using Microsoft Windows reso	ources by means of Administra	ation Server	
I Using Microsoft Windows reso	ources by means of Update A	gents	
Do not install application if it i	is already installed		
	o an oady motanou		

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

🔳 Re	emote Installation Wizard	×
G	Remote Installation Wizard	
	Selecting action if operating system restart is required during installation	
	Select the action that will be performed if application installation requires an operating system restart.	
	C Do not restart the computer	
	Restart the computer	
	Computer will be restarted automatically	
	• Prompt user for action	
	User will be prompted to restart computer Prompt will appear every 5 minutes Computer will be restarted after 30 minutes	
	Modify	
	Force dosing the applications in blocked sessions	
	Next	Cancel

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

Page 20 | 47

## KASPERSKY B

<b>3</b>		
CNTEST(Administrator		ad prijec
Password:	••••••	or trop
	OK Cancel	
	CNTEST/Administrator Password: Confirm password:	CNTEST\Administrator Password: Confirm password: OK Cancel

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

Ren	bte Installation Wizard	×
9	Remote Installation Wizard	
:	arting installation	
	Click Next to start deployment.	

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

(=)	Remote Installation Wizard		
	Starting installation		
	The deployment has successf	ully started.	
	<ul> <li>Deployment task created</li> </ul>		
	💞 Deployment task started		
	Click Next for details.		
			Next
			Next
for specific c	omputers		Next
for specific c e defined for specific computer for case, use group tasks.	omputers Fr. We there tails for computers that are not included in ad	metatolen grape or for computen induktel in one or more	Next
for specific c softeed for specific corpus to defined for specific corpus the case, use group table. a task ak from file	omputers rer. Use these tails for computers that are not included in ad	metasten graps of for computers included in one or more.	Next
for specific c a defined for specific crops her cases, use group tasks. a task ak from file	omputers inter these tasks for computers that are not included in ad	methation groups or for computers included is one or more	Next
for specific c a defred for specific corpus de de d	omputers Inter. Use these tasks for computers that are not included in ad	mathation groups or for computers included is one or more Deploy 105 MDM mobile device server (10.1.254)	Next
for specific c	omputers ters. Use these tasks for computers that are not included in ad Application (Application 0.1.251) Sayonity Security Cartee Advantageous Serve	ministration groups or for computers included in one or more  Paylow 305 HBM making devices server (18.1.254) Task types: Total application schereb	Next
for specific c address to specific status a status a task a transfer	omputers rers. Use these table for computers that are not included in ad Application 0.1.250 Lagoridy Society Center Administration Server	methation groups or for computers included in one or more Deploy OS FION making devices server (10.12.54) Task type: Total application remain Application: Resperity Society Conter Admeniation Serve	Next
for specific c a drived for societ conver- ber cases, use group tasks. a task drivenfile	omputers ens. Use these tasks for computers thet are not included in ad (Application 0.1.254) Exagensity Security Carter Administration Series	methation groups of for computers included in one or more Deploy US MOM models device server (181.254) Task type: Total application remote Applications: Topperly Source (Center Admeniation Serve	Next
for specific could be added to specific could be added to specific could be the could be added to specific could be added by the specific could by the speci	omputers ens. Use these tasks for computers thet are not included in ad (Application 0.1.254) Regardly Security Carter Administration Serie	metastere groups of for computers included in one or more Deploy US MOM models device server (18.1.2.54) Task type: Total application remote Applications: Tasperity Society Conter Admetistration Sorre	Next
for specific of a shift of to specific or to the coses, we prove to the a lask a lask ak from the HEM mubble device server (	omputers es. Los these tails for computers thet are not included in ad ( Agolication 0.1.264) Regardly Security Center Administration Serie	metasteru giruppe of for computers included in one or more Deploy US MOM multific device: server (18.1.2.54) Task type: Total application: remote Applications: Tasperiry Sourcity Conter Administration Sovie	Next

10. 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

Kaspersky Security Center				
File Action View Help				
🗢 🔿 📶 🖬 🖬				
Kaspersky Security Center  Administration Server SECURITY-CI  Managed computers	Getting s	tarted » Administration	Server SECUR	ITY-CENTER » Mobile Device Management
Administration Server tasks Tasks for specific computers User accounts Computers Computers Computers Computers Computers Computers Control installation Certificates Certificates	Mobile Device Manage Moble Device Management and inventory on th computers within administration groups. Subfol View list of mobile devices ↓ Add/Remove columns ↓ Refresh	ement ne network. The folder contain ders contain lists of managed i	ns Kaspersky Lab I mobile devices.	Nobile Device Management services installed on
Unassigned devices     Repositories				Server:
	Application	Server add 👻	Version	iOS MDM Mobile device server
	OS MEM Mobile device server Export list	MDMSERVER	10.2.434	Product version: 10.2.434 Server address: MDMSERVER
	Properties			<ul> <li>Switch to computer in administration group</li> <li>Properties         <ul> <li>Assign profiles to mobile devices</li> </ul> </li> </ul>
Nobile devices servers: 1				

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)

Page 23 | 47

# KASPERSKY B

🔜 iOS MDM Mobile device server applic	cation settings	? <u>-                                   </u>
Sections	Certificates	
General Configuration profiles Provisioning profiles Managed applications Certificates Settings Events Advanced	Apple Push Notification certificate: Name: Manufacturer: Expires on: IOS mobile devices server certificate: Name: mdmserver.abc.lab Manufacturer: Kaspersky IOS MDM Server CA N1234 Expires on: Thursday, January 02, 2025 10:20:44 AM Ir	nstall
	Client root certificate: Name: sc.abc.lab Manufacturer: sc.abc.lab Expires on: Saturday, January 04, 2025 10:16:52 AM	
Help	OK Cancel	Apply

3. Click the Create CSR button:

equest new APNs certificate	
Please go through all the steps to request and retrieve a ne	# APNs certificate.
- Charles - CCD	Learn
Step 1, creating a CSK: To create a request of a certificate, click the "Create CSR required data, and save the request file to disk.	"button, enter the
	Create CSR
upload the the created at the first step to portal https://companyaccount.kaspersky.com and perform the sign CSR. Note that CSR signing functionality becomes av you upload to the portal a key that enables the use of MC Management) solution.	actions required to ailable only after M (Mobile Device
Step 3, requesting the public key of the APIIs certificate:- upload the file signed at the second step to portal https://dentity.appie.com/publicity.then save to disk th by the portal. You will need an Appie 2D to log in to the por retrieve one on https://appieid.appie.com.	e certificate created ortal; you can
-Step 4, conditing the CSR To complete the recuest, clok the "Complete CSR" button certificate retrieved at the third step.	and specify the Complete CSR
Inst	Cancel

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

Create CSR	×
Name:	
Nik	
Company:	
ABC	
Department:	
Π	
City:	
Moscow	
State:	
1	
Country:	
Russian Federation	<b>T</b>
	Save Cancel

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!

Request new APNs certificate
Please go through all the steps to request and retrieve a new APNs certificate.
Learn
- Step 1, creating a CSR:
To create a request of a certificate, cick the "Create CSR" button, enter the required data, and save the request file to disk.
Create CSR
Step 2, signing the CSR:
Upload the file created at the first step to portal <u>https://companyaccount.kaspersky.com</u> and perform the actions required to sign CSR. Note that CSR signing functionality becomes available only after you upload to the portal a key that enables the use of NDM (Mobile Device Management) solution.
Step 3, requesting the public key of the APNs certificate:
<u>https://identity.apple.com/pushcert</u> , then save to disk the certificate created by the portal. You will need an Apple ID to log in to the portal; you can retrieve one on <u>https://appleid.apple.com</u> .
Step 4, completing the CSR:
To complete the request, click the "Complete CSR" button and specify the certificate retrieved at the third step.
Complete CSR
Instell

Page 25 | 47

#### 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)

A ttps://companyaccount.kaspersky.com/arsys/shared/login.jsp?/arsys/	ည္ – 🔒 ငံ 🎯 Kaspersky Lab Customer Se × 🔐 🏠 🛱			
Welcome to CompanyAccount	KASPERSKY			
	Please log in.			
	Email Password Log In Clear Control of Clear			
Registration         Forgot your password?         FAQ for CompanyAccount           Kaspersky CompanyAccount is a special system designed for users of business products. The system allows sending and tracking the requests to various Kaspersky Lab departments: Technical Support service, Virus Lab, etc.         FAQ for CompanyAccount				
Based on the licenses, all employees of one organization are united by one CompanyAccount. This enables shared management of all requests and licenses of the organization and independent management of user accounts within a single CompanyAccount (after the corresponding privileges are granted).				
The number of user accounts per organization supported by CompanyA	ccount is unlimited.			
For details about CompanyAccount, please visit <u>http://support.kaspersk</u>	y.com/fag/companyaccount_help.			
If you are using software for home / small business, such as Kaspersky Kaspersky My Account.	Internet Security or Kaspersky Small Office Security, please, go to $\checkmark$			

Kaspersky My Account.



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)

	🖌 🏠 🕨 Search		
Requests	Services		1-4 of 4 <pn< th=""></pn<>
Your response needed     0       In Progress     0       Resolved     0       Inactive     19	Technical Support request Issues with Kaspersky Lab products, banner ads, phishing, and other web content related issues.	Send suspicious file for analysis If it contains an unknown malicious program, that will be added to antivirus database.	CSR Signing CSR Signing for Apple Push Notification Service
Submit Request Manage Users Manage Personal Information Manage License Information	CompanyAccount Question Submit an issue with CompanyAccount or provide feedback.		

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

	🖌 🏫 🕨 Search	<b>Γ</b> α	
Requests	Services		1-4 of 4 🔤
Your response needed     0       In Progress     0       Resolved     0       Inactive     19	Technical Support request Issues with Kaspersky Lab products, banner ads, phishing, and other web content related issues.	Send suspicious file for analysis If it contains an unknown malicious program, that will be added to antivirus database.	CSR Signing CSR Signing for Apple Push Notificato Service
Submt Request Manage Users Manage Personal Information Manage License Information	CompanyAccount Question Submit an issue with CompanyAccount or provide feedback.		

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

CSR Signing (cssapp) - Intern	et Explorer		×		
🎯 https://companyaccount.kaspersky.com/arsys/forms/cssapp/ISS%3ASRS%3AAdvancedInterface_C 🔒					
K lait lait					
CSR Signing for Apple Push Notification Service					
How to generate an APNs					
File Name	Size	Description			
		CSR Attachment			
Browse					
Sign CSR Cancel					

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:



Page 28 | 47

7. 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)

	🔹 🏠 🕨 Search					
			<b>↓</b> Q,		Knowledge	Base
Requests	Requests	View All requests		✓ Your requests	•	* Refre
Vour response needed 0	Resp Request ID Source	Summary	Status S	Status Reason Submission Date	Submitter Branc	Preferences -
Resolved 0	REQ000005472 CompanyAccount	t CSR Signing	Closed	9/30/2014 4:0330 PM 9/30/2014 6:38:03 PM 9/20/2014 5:04:02 PM	1	
	RE000003441f CompanyAccoun RE00000032441f CompanyAccoun	t CSR Signing	Closed	7/9/2014 4:22:34 PM 7/9/2014 1:39:50 PM	1	
Submit Request Manage Users	REQ0000030007; CompanyAccoun REQ0000027224; CompanyAccoun	t CSR Signing t CSR Signing	Closed	5/5/2014 4:11:08 PM 2/15/2014 7:39:49 PM		
Manage Personal Information Manage License Information	Summary For: REQ00	0003820195				🖹 Histo
	Status: Subject CSR Signing Detailed description A CSR signing re Service.	Closed	Request History: 12/4/2014.4:10: CSR Signed Your Cortlicate is Notification sorvi download link th (press "View File	35 PM : Alexandra Pryadko Signing Request (CSR) required to o was exceedingly signed. You ca at can be found in the request his y/petails" button) .	obtain an SSL certificat an downbad it any time tor y REQ00003820195	+ for Apple Push by following the support request

8. 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.

	Max Size	Attach Label	
ycert.plist	10 KB	File 1	
Display Save to	Disk		
	Maria da Davida		
	LAIEVandra Prvacko		
mitted by	Alexandia Figladita		
mitted by e of submission*	12/4/2014 4:10:35 Ph		

The file that is save is mycert.plist -

9. 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

🔒 Apple Ir	nc. [US] https://idmsa.apple.com/	IDMSWebAuth/logir	n?appIdKey=	3fbfc9ad8dfed	eb78be1d37f645	8e72adc3160d1	ad5b323a9e5c5
GoToMeeting	Kaspersky Internet S						
		Ś	Store	Mac	iPhone	Watch	iPad

Apple Push Certificates Portal

Apple ID	
Forgot your Apple ID?	
Password	
Forgot your password?	

2. In the next screen, click Create a Certificate

https://identity.apple	.com/pushcert/					
🗯 Store	Mac iPod	iPhone	iPad	iTunes	Support	٩
ple Push Cer	tificates Porta	al				Sign o
Certificates for	Third-Party Se	rvers		Create	e a Certificate	
Service	Vendor	Expiration Date*	Status	Actions		
Mobile Device Management	Fiberlink Communications	Oct 5, 2015	Active	Renew	Download	Revoke
Mobile Device Management	Laboratoriya Kasperskogo ZAO	Jan 4, 2016	Active	() Renew	Download	Revoke
Mobile Device Management	Laboratoriya Kasperskogo ZAO	Jan 15, 2016	Active	Renew	Download	Revoke
Mobile Device Management	Laboratoriya Kasperskogo ZAO	Feb 11, 2015	Revoked	() Renew		
Mobile Device Management	Laboratoriya Kasperskogo ZAO	Feb 26, 2015	Revoked	() Renew		
Mobile Device Management Mobile Device Management	Laboratoriya Kasperskogo ZAO Laboratoriya Kasperskogo ZAO	Feb 26, 2015 Feb 26, 2015	Revoked Revoked	<ul><li>Renew</li><li>Renew</li></ul>		
Mobile Device Management Mobile Device Management Mobile Device Management	Laboratoriya Kasperskogo ZAO Laboratoriya Kasperskogo ZAO Fiberlink Communications	Feb 26, 2015 Feb 26, 2015 Oct 5, 2015	Revoked Revoked Revoked	Renew     Renew     Renew     Renew		



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:





5. Next, click Download and save the MDM\_Laboratoriya Kasperkogo ZAO\_Certificate.pem file



6. 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.

Page 32 | 47



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



5. 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:

Enter data for certificate	X
Friendly name for certificate:	
ABC Lab APNs certificate	
Password:	
•••••	
Confirm password:	
•••••	
OK Cancel	

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

Request new APIIs certificate
Please go through all the steps to request and retrieve a new APNs certificate.
Learn
Step 1, creating a CSR:
To create a request of a certificate, cick the "Create CSR" button, enter the required data, and save the request file to disk.
Create CSR
Step 2, signing the CSR:
Upload the file created at the first step to portal https://companyaccount.kaspersky.com and perform the actions required to sign CSR. Note that CSR signing functionality becomes available only after you upload to the portal a key that enables the use of MDM (Mobile Device Management) solution.
Upload the file signed at the second step to portal https://identity.apple.com/pushcert, then save to disk the certificate created by the portal. You will need an Apple ID to log in to the portal; you can retrieve one on https://appleid.apple.com.
Eten 4. completion the CEU
To complete the request, click the "Complete CSR" button and specify the certificate retrieved at the third step.
Complete CER
Install

Page 34 | 47

IOS MDM Mobile device server appli	cation settings	<u> </u>
Sections	Certificates	
General Configuration profiles Provisioning profiles Managed applications Certificates Settings Events Advanced	Apple Push Notification certificate: Name: APSP:580ecc1a-6040-4ce7-93a0-4cbc0851649d Manufacturer: Apple Application Integration Certification Authority Expires on: Tuesday, January 05, 2016 10:55:01 AM Request new IOS mobile devices server certificate: Name: mdmserver.abc.lab	Inetal
	Manufacturer: Kaspersky iOS MDM Server CA N1234 Expires on: Thursday, January 02, 2025 10:20:44 AM	Install
	Client root certificate: Name: sc.abc.lab Manufacturer: sc.abc.lab Expires on: Saturday, January 04, 2025 10:16:52 AM	
Help	OK Cance	Apply

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

KASPERSKY	Search	Q	Register Sign in
PRODUCTS & SERVICES	ONLINE SHOP INTERNET SECUR	TY CENTER TRIALS & UPDATES	UPPORT PARTNERS ABOUT US
			English (Global)
Home Support Kaspersky	Security Center 10		
i≣ Product Select	Kaspersky Security Cent	er 10	
Knowledge Base			Total Mandan
Downloads & Info	Status: Supported	Download:	
System Requirements	Database Update	Documentation	×
Common Articles	Error fix	What is this a Administrator Guide [.pdf	, 3.4 MB]
How-to Videos	Latest Version: 10.2.4	H Databas Getting Started [.pdf, 934 Implementation Guide [.p	L4 KB) df. 1.5 MB]
Forum	Commercial Release date: 30 January 201	3 device) User Guide (Web-Console	][.pdf, 1.5 MB]
Contact Support		Support Download	
Safety 101		Error for Release Full package: <u>ksc10.2.434</u>	lite_en.exe [123.8 MB] & MD5 ien.exe [871.1 MB] & MD5
		Packages for remot	e management
		Web Console (Version 10	0.110): 0.110 Data and TXE 4 MMT
For Software Users	Free online courses	For Linux (rpm) x86: ksg	webconsole-10.0.110-10.en.i386.rpm [5.7 MB]
		For Linux (rpm) x64: Ker	webconsole 10.0.110-10.en and64.deb [5.7 MB]

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

🕙 Kaspersky Security Center V	/eb-Console 10.0 Setup 💼 💼 💌
	Welcome to the Kaspersky Security Center Web-Console 10.0 Setup Wizard
	This wizard will unpack the installation files of Kaspersky Security Center Web-Console 10.0 to your computer.
	Click Next to continue.
R	
	Next > Cancel

Page 36 | 47



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

4.	
📀 Kaspersky Security Center Web-Console 10.0 Setup	
Select destination folder Select the folder, to which Kaspersky Security Center Web-Console 10.0 files will be unpacked.	<b>F</b>
This wizard will unpack Kaspersky Security Center Web-Con: To unpack to another folder, click Browse and select anothe unpacking.	sole 10.0 to the specified folder. r folder. Click Install to start
Destination folder C:/kscwc_10.0\en	Browse
Space required: 18.4MB Space available: 183.4GB	
< Back	Install Cancel

The expander continues:

📀 Kaspersky Security Center Web-Console 10.0 Setup		
Copying files Please wait, while copying Kaspersky Security Center Web-Console 10.0 files		
Extract: apache.exe 83%		
< Back	Close	Cancel

Compute + Local Dek (C) + Kons (D + on + WebConsole + 4)
 Soreh HieldConsole

 Console - 4)
 Soreh HieldConsole

 Provide

 Prov

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

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



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

Kaspersky	ecurity Center Web Co	nsole Setup	
Custom Se	tup		
Select the	way you want features to b	e installed.	
	Kaspersky Lab Web Intern Kaspersky Lab Self Service	ace Portal	
Kaspersky Lab	Web Interface		
This feature re	quires 1KB on your hard dr	ive.	
ocation:	C:\Program Files (x8	6) (Kaspersky Lab (Kaspersky	Browse
	Security Center Wel	o-Console \	Dioviseri
			_
		Back Next	Cancel

Page 38 | 47

- Installing Apache Server

   Select Apache server installation.

   Install Apache HTTP Server 2.2

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

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

🙀 Kaspersky Security Center Web Consol	e		<u> </u>
<b>Certificate for Working via HTTPS</b> Select a certificate.			
A certificate signed by an official cer	tification center s	hould be used.	
• Create new certificate			
C Choose existing			
Select certificate file;			Browse
Select a private key:			Browse
To start Apache installation, click the Next but the installation process. Kaspersky Security C completing this operation.	tton. Restart of c enter Web Conso	computer may b le installation v	e needed during vil continue after
	Back	Next	Cancel



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:

🙀 Kaspersky Security Center Web Consol Configuring the installation of Apac	e <b></b> ×
Specify instalation settings.	
Domain name:	abc.lab
Server name:	192.168.2.100
Administrator's email address:	admin@abc.lab
	,
	Back Next 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:

🙀 Kaspersky Security Cent	er Web Console	- 🗆 🗵
Selecting Ports Specify the required ports		
Enter the Administration Se 65535.	rver SSL port. Port numbers must be within the range of 1	1 to
SSL port number:	13291	
Enter a port number to acc of 1-65535.	ept connections from Apache. The value must lie in the rai	nge
Port number:	9000	
Select computer where Adn	inistration Server is installed.	
Server address:	10.28.0.20 Connection gateway	
	Back Next C	ancel



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

👘 Ka	spersky Security Cent	er Web Console Setup	- 🗆 🗵
Se	electing Ports		
	Specify the required ports		
Er 61	nter a port number for We 5535.	b Console. The value must be within the range 1 through	
P	ort number:	8080	
Er th	nter a port number for Sel prough 65535.	Service Portal. The value must be within the range 1	
P	ort number:	8081	
		Back Next Ca	ncel

13. 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:

🖶 Kaspersky Security Cent	er Web Console Setup	×
Account for Self Service Port	al	
User must have rights to rea	ad and connect new devices to Self Service I	Portal.
User name: Password:	ABC\Administrator	Select
Server name:	http://192.168.2.100	
	Back Next	Cancel





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 <a href="http://localhost:8081">http://localhost:8081</a>. 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) Apple Push Notification Google Cloud Messaging (GCM) Services (APNs) MDM profile Ŷ Is installed on an iOS device, enables MDM for iOS remote management: locking, installing programs iOS Safe . Safe Bro Browser A secure browser

with Web protection ..... KES for Android Mobile KES for Mobile A protection and remote management tool, including anti-. . . .

### **ADMINISTRATION SERVER - CONNECTIONS**



٥

Mobile devices support

ፈ..

KSC

Administrat Server

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

virus

### **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

Page 45 | 47



Safe Browser

### **IOS DEVICES - CONNECTIONS**

iOS

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)



Page 46 | 47

#### Appendix: iOS client details

### iOS MDM Management – Component Details

