Introduction

With the release of Kaspersky Security Center 10.0 a new functionality has been implemented which allows centralized management of mobile devices running various operating systems (Apple iOS, Android, Blackberry, Symbian, etc.) from one single location. Now, in addition to agent-based solution (called Kaspersky Security for Mobile), an agent-less MDM is available. This mobile device management (MDM) solution operates by integrating with existing IT infrastructure solutions like Exchange ActiveSync or Apple Push Notification service and making use of these technologies to provide a single place to manage thousands of devices.

This document describes all steps required to setup a proper MDM-environment and integrate it with Kaspersky Lab solution.

It is divided on 3 deployment parts:

1. Kaspersky Lab Mobile Device Management with Microsoft Exchange Active Sync (agentless)

2. Kaspersky Lab Mobile Device Management with Apple MDM Server (agentless)


Each part has some milestones to complete to deploy MDM solution in a test-lab or production environment. The description of installation prerequisites (hardware and/or software requirements) is provided at the beginning of each part.
Kaspersky Lab Mobile Device Management with Microsoft Exchange Active Sync

About Kaspersky Lab MDM through Exchange Active Sync

The new feature introduced in Kaspersky Security Center 10 is the ability to see mobile devices in KSC console and to be able to manage Microsoft Exchange ActiveSync device profiles through Kaspersky Security Center. The actual enforcement of profile settings is done by Microsoft Exchange.

Prerequisites

You can use any virtualization software you wish to or deploy this solution to non-virtual environment, provided that your configuration meets the specifications described below. Also, due to some virtual environment constraints, an Android virtual device has been implemented on host machine (Microsoft Windows 7) in this configuration with Android SDK and Java being used for virtual android device deployment. It is recommended to use any supported non-virtualized Android device to test this deployment scenario.

Hardware & software requirements:

This deployment requires a minimum of 2 servers and 1 mobile device with hardware and software specifications provided below:


   **Hardware specifications:** CPU x64 processor, 2 GHz+, 4GB RAM, 100 Gb HDD (NTFS partitioned)


3) 1 or more mobile devices that support following operating systems:

   - Windows Phone
   - Apple iOS
   - Android
   - BlackBerry
   - Symbian
   - etc.


Please, note that this document addresses Kaspersky Lab products deployment and configuration only on Android and Apple iOS devices. Other mobile OSs from the list above are also supported by Kaspersky Lab products mentioned in this document (where applicable) and have their configuration similar to what is described for Android and Apple iOS devices.
Deployment


Before you begin your MDM deployment, ensure KSC10 is installed with all required MDM plugins and all necessary features:

During installation ensure to select “Mobile devices support” as well as the following components:

We will not describe all the rest KSC10 deployment steps here. Please, refer to KSC 10 Implementation Guide. If you don’t have a KSC10 server deployed, please install it on a separate Microsoft Windows Server machine joined to local domain or install it to your DC instead.


In this document, Microsoft Exchange Server 2010 64 bit platform is used for demo purpose. It is allowed to use any other available product version that supports ActiveSync.

If there is no deployed Microsoft Exchange Server, install it with Client Access, Hub Transport and Mailbox roles. Install an Edge Role. If an existing Microsoft Exchange Server is used, please, re-configure it with the required roles.

It is recommended to use Microsoft Exchange 2010 with Microsoft Windows Server 2008 Enterprise Edition 64bit. Create a new Microsoft Exchange server forest to provide email services for your domain or use existing one. Add a test user mailbox mobile devices will connect to (i.e. tomas@vlab.local used here). Enable Active Sync for this mailbox via Exchange Management Console (in either case, Kaspersky Lab product will not work). Create as many test user mailboxes as required, or use production ones.

Deploy Network Agent to dedicated Microsoft Exchange Server (which is used for MDM in your environment) through either of methods available (remote installation from KSC server, local installation, etc.). Run klcnsntgui.exe utility to ensure NA is connected to the correct KSC server from which you are planning to manage mobile devices. If NA points to wrong Kaspersky Security Center (KSC) server then MDM server will not be available in KSC console.


Before installing the actual Kaspersky Lab MDM component for Exchange (used for integration), ensure you enable Windows Authentication for your Exchange 2010 server site.

Start IIS Manager and drill-down to Default Web-Site. Enable Windows Authentication for PowerShell virtual directory.

Copy the MDM installation files folder located in where KSC10 extracts installation files (usually C:\ksc10.0\en\MDM4Exchange) to Exchange Server and run setup.exe. Follow the on-screen instructions to setup Exchange MDM Server:
On Welcome screen click Next and accept the License Agreement. Click Next.

Select Standard mode (default) if you run stand-alone server, or Cluster mode if you run Exchange cluster and click Next. Kaspersky Lab product supports installing on Exchange cluster:

If you select Cluster Mode no further configuration is required, continue with steps described below. Provide the account for managing product with administrative permissions on Exchange Server. Click Next:

Provide an URL for Remote PowerShell connection. Click Next.
Click the **Install** button to start the installation.

![Exchange ActiveSync mobile devices server](image)

**Note:** You can install **Kaspersky Exchange MDM Server** component by any other available means (i.e. creating a **Kaspersky Lab** application installation package in **KSC10 Console** or using **3rd party deployment solution**).

After **Exchange MDM** component is installed, switch back to **Kaspersky Security Center** and start it. Under **Mobile devices** your new **Mobile Device Server** should appear.

![Kaspersky Security Center](image)

If it’s not – ensure you properly installed **network agent** and it successfully connects to **KSC10 server** with **MDM**. If **NA** points to another **KSC** server, which is unavailable, it will not transfer any **MDM** data to your **KSC** server. In this case, use **klmover** tool to point **NA** to the correct server.

**Note:** If you don’t see the **Mobile Devices** menu option, click the **Administration Server** in the left pane and select **View -> Configure Interface**. Select “Display mobile devices management” check-box.

![Configure interface](image)

You can also validate successful **MDM Server** installation by browsing to **Managed Computers**, selecting the client with **MDM server** installed (if it’s not in a **Managed Computers** group, move it there manually) and clicking **Properties**. Ensure that **Applications - Managing mobile devices via Exchange server** has status **Running**.
Click **Properties** and select **Mailboxes**. A list of **Microsoft Exchange** mailboxes will appear.

You can now manage **Exchange** mailboxes and profiles. Start by creating a new profile and assigning it to test user mailbox -  **tomas@vlab.local**.

In this document we describe managing an **Android virtual device** via **Microsoft Exchange Active Sync**. Other OSs’ settings related to **Active Sync** deployment may depend on that specific OS, but these settings are similar and identical in most senses.

5. **Configure Android device to connect to Exchange Active Sync.**

In this document **Android 4.0.3 version** configured as a virtual device has been used.

Start your **Android device** and launch **Email application** (install it if it is not already installed on Android device).

Click **Email**. An **Email Client** will start. **Account setup** page will appear. Start typing account name and **Manual setup** button will appear shortly. Click **Manual setup**.
On next page click **Exchange** account:

On next screen type the details – **Domain\Username, Password** and provide **Server** name:
Click **Next**. Wait a few seconds until the following message appears:

![Remote security administration](image)

Click **Ok** and move on to the next page. Here you allow **Exchange server** to manage security settings on device.

![Account settings](image)

Click **Next**. Activate device **Administrator** screen will appear. Click **Activate**

![Activate device administrator?](image)
Wait for the final screen to appear and click **Next:**

After this step synchronization of **Android device** with **Exchange ActiveSync** is complete.

Before proceeding to the next step, ensure your device is connecting to **Exchange Server**. A security warning may appear that states “**Could not open connection to server due to security error**”. Swipe down the screen and open this system message. Click **Ok**.

If you already configured a profile with password settings, the following screen will appear:
Click Password and type a new password for your account

Click **Continue**. Confirm your password and click Ok.

After this step click on sync button in **Email application** interface and wait for initial sync to complete. You may notice the following warning:

In this case, switch to your **Exchange Server**, open Exchange Management Shell, browse to **Recipient Configuration** and enable **Active Sync** for your test user mailbox (**tomas@vlab.local**). After this you’ll be able to sync user’s email.

You can now successfully sync with **Exchange Active Sync** powered by **Kaspersky Security Center 10**.

**6. Create Exchange ActiveSync profile using Kaspersky Security Center**

Next step is to set up a profile through the means of **KSC10 server**. Open **KSC10** and navigate to **Mobile Devices** -> **Mobile Device Servers**. Click **Assign profiles to mobile devices** button.
Use **Change Profiles** button to create a new profile. A window with **Default Profile** will appear.

![Image of Change Profiles window]

Click **Add**. A new window will appear. Provide a name for your profile and configure its settings.

![Image of profile configuration window]

Not all **Exchange ActiveSync** profile settings are copied to **KSC server**. Most settings that will definitely work on most devices are copied, but some features that are limited for use only on **Windows-based mobile devices**, will not be copied.

Create a profile that will have **password length complexity** setting set to the minimum of 8 characters.

![Image of profile with password length setting]

Click Ok and this will save profile. Then on **Mailboxes** screen select the mailbox **tomas@vlab.local** and click **Assign profile**. You will immediately see that **Profile in use** column populates with the profile you just assigned to this mailbox. Go to **Android device** and you will see that it is now managed. Open **KSC console** and go to **Mobile devices->Exchange ActiveSync mobile devices**. You will see **tomas@vlab.local** mailbox on the list connected.
You can view the detailed info on device by clicking **Properties:**

This finishes the first deployment part.

**Kaspersky Lab MDM with Exchange Active Sync synchronization scenarios:**

Depending on IT infrastructure where Kaspersky Lab MDM is deployed there may be various options on how to synchronize mobile devices with Exchange Active Sync. Let’s consider 3 of them:

1. Corporate users accessing local network resources through local wireless network
2. Mobile users connect to corporate resources via 3G network.
3. Mobile users connect to corporate resources from Wi-Fi hotspot.

Mobile devices do not connect directly to KSC10 server. Mobile devices connect to Microsoft Exchange server instead, as usual. As long as there is connection with Exchange Server, KSC 10 will sync settings and apply it to devices via Exchange ActiveSync profiles. There’s no need to separately route traffic from mobile device to KSC10 server in this deployment scenario. That is, when Exchange ActiveSync is successfully configured to support all 3 described scenarios and KSC10 is able to reach Exchange Server – the system is already setup, no further configuration is required here. If there’s a firewall between mobile devices and Exchange server (like in scenario 2 and 3), some ports need to be open to allow connection. Please, see the following Microsoft article for details:

http://support.microsoft.com/kb/259369
Kaspersky Lab Mobile Device Management with Apple MDM Server

About Kaspersky Lab MDM with Kaspersky Apple iOS MDM Server

In addition to ActiveSync mobile device management, Kaspersky Security Center 10 now has the feature to manage Apple iOS mobile devices, called Kaspersky Apple iOS MDM Server. In comparison to managing Apple iOS devices through Exchange Active Sync, this MDM technology provides more advanced security and management features especially for Apple iOS devices. Kaspersky Apple iOS MDM Server is required for this purpose, which can be deployed to Windows XP/Vista/7 machine or Windows Server-based OS (Microsoft Windows Server 2003/2008/2012).

Prerequisites

In order to manage Apple iOS devices, a separate MDM server is deployed. This server can be deployed as standalone, or on the same server as KSC10. Basically, the environment is the same as in Part 1 of this guide. It is recommended, however, to create a standalone Mobile Device Management server on different hardware or VM, different from Kaspersky Security Center 10 server or domain controller (DC). Apple Configuration Utility (iPhone Configuration Utility) is also required on host that is responsible for managing both KSC10 and MDM devices.

Deployment

1. Preparation

Install Network Agent on server acting as Kaspersky Apple MDM Server. It can be standalone, or mixed with other application servers. Proceed to the next step.

2. Local/Remote Apple MDM server installation

Open Kaspersky Security Center console, navigate to Remote Installation -> Installation packages.
Click **Create Installation package.** A wizard will start.

Provide a name for this package and click **Next.**

Select .kud file with **Apple MDM server.** It is located in folder where KSC unpacks installation files by default.

Upload the installation files to local server and start the remote deployment, selecting a separately configured **Apple iOS MDM server,** which is already deployed on 1st step.

If you deploy **Apple MDM server** manually (by copying files directly to remote host), follow the installation instructions provided here:
Launch the iOS MDM Server installer on the host:

Accept the Terms of License Agreement on next screen. Click Next. Provide the ports used for MDM connection.

Provide an URL for connection to MDM server.

Wait while the application installs.

When installation finishes, ensure that MDM server is visible under Mobile Devices Servers in console:
3. Create an APN certificate signing request.

APN stands for Apple Push Notification service – a special Apple service acting as an intermediate between Apple device (iPhone, iPad) and MDM server.

When an MDM server wants to communicate with iPhone or iPad, a silent notification is sent to the device via the Apple Push Notification service, prompting it to check in with the server. The process of notifying the device does not send any proprietary information to or from the Apple Push Notification service. The only task performed by the push notification is to wake the device so it checks in with the MDM server. All configuration information, settings, and queries are sent directly from the server to the iOS device over an encrypted SSL/TLS connection between the device and the MDM server.

In order to generate APN certificate you must have an access to Kaspersky CompanyAccount account and register Apple ID on Apple website.

A detailed guide on how to generate APN is provided here: http://support.kaspersky.com/9245

4. Install APN certificate to Apple MDM server.


On Certificates tab under Apple Push Notification certificate click Install. Select your new APN certificate and click Open. If everything is correct you should see the details with Name, Manufacturer and Expires on fields being populated.

5. Connecting iOS mobile devices to Kaspersky Apple MDM Server

After APN certificate is generated and installed users can connect their mobile device to Kaspersky Apple MDM Server. To allow them to do this, go to User Accounts tab in KSC10 Console, select mobile device users, right-click and select Install iOS MDM profile.
A new window will open with settings. Select your MDM server and choose notification methods (via SMS or via Email). Provide a Notification message text:

Now, the last thing to do is to install a profile on users’ devices. The user needs to open a link on his or her mobile device and proceed with steps to install it. After profile is installed, new MDM devices will appear under iOS MDM mobile devices list in Mobile Devices pane in KSC10 console.

6. Manage Configuration and Provisioning profiles

After you successfully setup APN certificate, you can start managing Apple iOS devices from KSC10 console. This can be done via 2 types of profiles – configuration profiles and provisioning profiles. For provisioning profiles – see this article [http://support.kaspersky.com/9783](http://support.kaspersky.com/9783)

Both profile types are accessible by navigating to Mobile devices -> Mobile devices servers -> iOS MDM mobile devices server.
Profiles can be assigned to any **iOS device**, provided that it is visible.

**Apple Configuration Utility**

Apple has enhanced and locked down the security of mobile devices. To be able to edit configuration profiles, a special utility is required on each host, which is used for MDM management (KSC Console), called **Apple Configuration Utility**.

This utility can be found under following link: [http://support.apple.com/kb/dl1466](http://support.apple.com/kb/dl1466)

Profiles can be applied based on specific device’s user. To apply a profile this way, navigate to **User Accounts** tab and select the mobile device user.
Click **Install iOS MDM profile to user’s mobile device.** The following window will appear. Configure required settings and click Ok.

The profile will be applied immediately.

**Apple Push Notification network setup**

When **MDM servers** and **iOS devices** are behind a firewall, some network configuration may need to take place in order for the MDM Service to function properly. The following ports need to be open for firewall connections between **Kaspersky MDM Server** and **APN Service**:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9799</td>
<td>TCP</td>
<td>Send notifications from APN Service to MDM Server NA</td>
</tr>
<tr>
<td>9899</td>
<td>TCP</td>
<td>Send notifications from MDM Server NA to APN Service</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>External port to connect mobile devices to APN Service.</td>
</tr>
</tbody>
</table>
# Kaspersky Lab Mobile Device Management with Kaspersky Security 10 for Mobile

*Not all features are supported in all versions of mentioned OS*

<table>
<thead>
<tr>
<th>Feature</th>
<th>ANDROID</th>
<th>IOS</th>
<th>SYMBIAN</th>
<th>WINDOWS MOBILE</th>
<th>BLACKBERRY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANTI-MALWARE FEATURES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-virus scanning of files as they are opened, saved, or executed</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Scanning of new apps after installation</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Heuristic scanning during protection</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Mobile device protection against network attacks via TCP/IP</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td><strong>PRIVACY AND ANTI-THEFT FEATURES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocking of the unwanted incoming calls and SMS</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Possibility to get the current phone number via SMS or e-mail when the SIM card is replaced or ejected</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Possibility to lock the device remotely if it gets stolen or lost</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Possibility to wipe user data remotely if the device gets stolen or lost</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Possibility to wipe all device data remotely</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Possibility to determine device coordinates remotely</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Encryption of files</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td><strong>CONTROL FEATURES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocking of malicious and phishing web sites (by default) and web site filtering by administrator-specified categories</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Management of installed apps on devices via Kaspersky Security Center</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Creation of a list of allowed, prohibited apps and the required apps.</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td><strong>Corporate data protection with the containers</strong></td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Detection of root privileges or jailbreak on devices</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td><strong>DEPLOYMENT OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Via Email</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Via SMS</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Via “App Store”</td>
<td>PLANNED</td>
<td>PLANNED</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Via Workstation</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Via MDM</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Local installation on a device</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
About Kaspersky Lab MDM with Kaspersky Security 10 for Mobile

In addition to agent-less features, provided by integrating KSC10 with Microsoft Exchange ActiveSync and Apple iOS MDM Server, a legacy agent-based technology is still available through KS 10 for Mobile solution.

Please, see the latest release notes regarding Kaspersky Security 10 for Mobile on the following link: [http://support.kaspersky.com/9613](http://support.kaspersky.com/9613)

In this document Android mobile device management with KS 10 for Mobile is described. Please, be aware that the latest product version supports other mobile OSs, like Symbian, Win Mobile, Apple iOS, Blackberry. Installation on these OSs is beyond the scope of this document.

We will consider 1 deployment model (see Application deployment models for Android devices on page 15 of KS 10 for Mobile Implementation Guide) here. For other deployment options (SMS) on other supported OSs (Win Mobile, Symbian, Blackberry), please see the documentation – KS 10 for Mobile Implementation Guide.

Prerequisites

Agent-based MDM with KS for Mobile requires at least 2 servers for deployment: one is KSC10, the other is a domain controller. Email server with configured recipient list is also required (i.e. Exchange server used in previous setups). It is recommended to deploy the same server configuration as used in Kaspersky Lab Mobile Device Management with Exchange Active Sync part. KS for Mobile deployment via email requires a configured email server with recipients (mobile device users), who will receive an email with a link to download KS for Mobile product distribution package and run the setup.

For this document we used Android 4.0.3 OS device installation.

For other supported mobile OS versions, please, see the document: [http://support.kaspersky.com/ks10mob#requirements](http://support.kaspersky.com/ks10mob#requirements)

Deployment

1. Preparation.

Start your domain controller (DC), KSC10 server and Exchange server. Download the distribution package from Kaspersky Website [http://support.kaspersky.com/ks10mob#downloads](http://support.kaspersky.com/ks10mob#downloads) -> Package for Security Center.

2. Enable mobile devices support on KSC10 server

Open KSC10 Server console and right click Administration Server -> Properties. On Settings tab ensure Open port for mobile devices setting is enabled. Leave the default port 13292.
3. Create KS 10 for Mobile installation package (Android)

Open Remote Installation -> Installation packages. Click Create installation package. A new window will open.

![Create installation package window]

Click Create Installation package for a Kaspersky Lab application. Provide a name for this package (i.e. MDM Mobile) on next screen. Click Next.

![Select distribution package]

On Selecting the distribution package for installation page click Select and browse to the folder where you extracted sc_package_en.exe archive (C:\KAV\KSM10). Click kmlisten.kpd and click Open. Click Next and start the upload process. Wait until all necessary files are uploaded. You will then see the package in the list of all installation packages:

![Installation packages list]

After this initial package is created, configure its settings by double-clicking MDM Android package or clicking Show installation package properties window in the right pane. On Properties window click Settings in the
left pane. Specify **Administration Server address** (or DNS name) and **SSL port number**, as well as the name of the group to allocate computers in (this group will be created automatically after first sync with **Administration Server**). Select **Request email address** if you want the user to be prompted for email address when he installs application to mobile device. Click Ok.

Now it is necessary to create a **stand-alone installation package** to deploy product to mobile devices. Select your newly created package **MDM Android** and click **Create stand-alone installation package**. A wizard will start in a new window.

Follow the wizard and **create stand-alone installation package**. Go back to installation packages window and select **View the list of stand-alone installation packages**. The window similar to this will open

Copy the URL to this package. Open your email application (i.e. **MS Exchange Outlook OWA**) or similar.
Email this link to users of mobile devices.

4. **Install Kaspersky Security for Mobile on Android**

Start your **Android** device and wait while it loads. **Open Email application**, connect to **Exchange server** with your test user account (**tomas@vlab.local**). If you emailed an installation link on the previous step, you should now see a message with a hyperlink to **download Kaspersky Security 10 for Mobile** application. If not – you can use **KSC10 automated system** to send emails to specific user accounts.

Emails can be sent by browsing to **User Accounts** tab, selecting an account and clicking **Send message by email**:

Click the hyperlink to download **Kaspersky Security 10 for Mobile** product. Start the installer after download completes:
Wait while installation finishes:

Start the application. Proceed with initial configuration.

Click **Continue**

Click **Disable**. You may notice the following message. It may appear if you already configured agentless **ActiveSync**.

Click **Deactivate**. On next page configure **Synchronization Settings**
This completes the initial configuration wizard.

Click *Start App*. You will see the default interface.
Ensure that device can see the **KSC 10 Server** and synchronize with it. Click **Additional -> Synchronization** to configure connection with **KSC10 Server** settings:

![Synchronization settings](image)

There's no need to go and modify sync settings. Just click **Synchronization** and you will see the following on your mobile device screen:

![Synchronizing...](image)

If synchronization attempt fails, please read the following article regarding sync with **Kaspersky Security Center 10**: [http://support.kaspersky.com/9793](http://support.kaspersky.com/9793)

As soon as synchronization occurs, configure the device and download necessary anti-malware updates.

Ensure that this new mobile device is visible in **KSC10**. Login to **Kaspersky Security Center Console** and go to **Managed Computers**. Open **Computers tab** and click **Add computers**.

![Add computers](image)

Drill down to **Unassigned computers**, find **KSM10 group** and select **tomas@vlab.local<id>**.
Your device should then be visible under **Computers tab:**

![Computers tab](image)

5. **Configure and apply Kaspersky Security for Mobile 10 Policy.**

Now, go to **Policies tab** and create a new policy called **Mobile Devices.**

![Policies tab](image)

Create this policy for **Kaspersky Security 10 for Mobile** product. This new policy will be immediately applied to your device.

![Policy creation](image)

This **Kaspersky Security 10 for Mobile** policy is single for all types of mobile OSs supported by product.

If connection to device is stopped for some reason the policy will be applied at next heartbeat.

This finishes the deployment process for **Kaspersky Security 10 for Mobile** on **Android** device using an email link.

**Using containerized application containers on Android device**

You can configure a container for your mobile device. Containerized application is application on mobile device that can be managed via security policy on **Kaspersky Security Center** server. For example, you can completely block application activities on all mobile devices. Let's see how it works.

1. Download application `.apk` file
2. Add `.apk` file to stand-alone installation packages list.

   Navigate to **Installation packages** and select **Manage packages of mobile applications.** A new window will open. Select new
A new package creation wizard will launch. Select this installation package you downloaded on first step and tick Create container with the selected app. Click Next.

Wait while the package uploads and finish the wizard. This new package should now be visible.

3. Create a container policies for a containerized application

Go to Managed Computers -> Policies tab. Double-click Mobile Policy. Click Containers on left pane
The following features are supported for security containers (Android and iOS):

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>This drop-down list lets you enable or disable authorization when an app is launched in a container on the user's mobile device</td>
<td>Disable. <strong>Kaspersky Security</strong> does not require the user to pass additional authorization when an app is started in a container. <strong>Domain credentials.</strong> When an app is started in a container, <strong>Kaspersky Security</strong> requires the user to pass authorization. The user must specify the domain login and password in <strong>Active Directory</strong>. The app will not start in the container without user authorization. <strong>User sets the password.</strong> When an app is started in a container, <strong>Kaspersky Security</strong> requires the user to pass authorization. The user must specify the password set at the first startup of this app in the container. The app will not start in the container without user authorization.</td>
</tr>
<tr>
<td>Data saving privileges</td>
<td>The Data saving privileges section lets you restrict the rights to save data of a containerized app on the user's device.</td>
<td><strong>Allow</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Allow before Exit</strong></td>
</tr>
<tr>
<td>Block copying data to other apps</td>
<td>Restricts data copying by a containerized app on the user's device.</td>
<td><strong>Enabled/Disabled</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If enabled, the containerized app is unable to copy its data to other apps on the user's device.</td>
</tr>
<tr>
<td>Internet Access</td>
<td>Restrict Internet access of a containerized app.</td>
<td><strong>Allow.</strong> Containerized application has full Internet access with no restrictions</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Prompt.</strong> Kaspersky Security notifies the user that containerized application is attempting to access Internet. The user is prompted for action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Block.</strong> Containerized application is not allowed to access Internet</td>
</tr>
<tr>
<td>Messages</td>
<td>Select a mode that restricts the sending of SMS by the containerized app.</td>
<td><strong>Allow.</strong> The containerized app uses the SMS gateway to send messages without restrictions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Prompt.</strong> Kaspersky Security notifies the user of the device that the containerized app is attempting to send an SMS and prompts the user for further action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Block.</strong> The containerized app is not allowed to use the SMS gateway to send messages.</td>
</tr>
<tr>
<td>Calls</td>
<td>Allows blocking a containerized app from receiving incoming calls</td>
<td><strong>Allow.</strong> The containerized app makes calls without restrictions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Prompt.</strong> Kaspersky Security notifies the user of the device that the containerized app is attempting to make a call and prompts the user for further action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Block.</strong> The containerized app is unable to make calls.</td>
</tr>
</tbody>
</table>
Configure these features similar to this screenshot:

![Screenshot of configuration settings]

4. Deploy containerized application to the device

Now open **Android device**, open **Browser** application and follow the link to installation package on **KSC** server (usually it is like `http://<KSC10server>.yourdomain.com:8060/dlpkg?id=<ID>`).

![Chrome app installation prompt]

Click **Install** and wait while it finishes. Launch application after installation. See what happens when you start **application** and what happens when you open websites. Also ensure that container policy is applied. If it is necessary – re-sync policy with server by clicking **Synchronization** in **Kaspersky Security 10 for Mobile Application**.

**Using containerized application on Apple iOS device.**

**Prerequisites**: a client must be a member of the Apple Developer Program (up to 100 devices) or the **iOS Developer Enterprise Program**.

To install a containerized application to **Apple iOS**, use **KSC 10** server and **KS 10 for Mobile** product. To deploy application, you first need to sign a distribution package for this application (in comparison to **Android OS**, where no signing is required).

Detailed information on how to sign a distribution package and upload an application to mobile device, using containerized application is described in the following article:

[http://support.kaspersky.com/9614](http://support.kaspersky.com/9614)

The configuration and features are similar to container configuration on **Android devices**.

**Note**: Not all Android and iOS applications can support containerization feature.