Kaspersky Mobile Device Management technologies

Mobile devices have become an integral part of our lives. Smartphone and tablet owners would be hard pressed to go without their devices even for a short time. According to data from Forrester Research, which conducted a study in late 2012, three out of every four employees want to use their personal mobile devices for work. This approach has become so widespread that it now has its own acronym: BYOD, or Bring Your Own Device. The practice is now supported in many companies around the world. In particular, one-third of the organizations surveyed in a different study conducted by B2B International in July 2012 allow their employees to connect personal smartphones to corporate resources

The advantages of the BYOD approach are obvious, as employees can work on devices that they are familiar with, and they can do that at home, in the office, or any other convenient location. However, there are also some downsides to BYOD — corporate information can be lost or leaked if a personal tablet or smartphone is lost or stolen, and connecting an infected device to a corporate network can lead to infection of the company's infrastructure.

In general, the risks associated with BYOD — and corporate mobile devices — can be put into two categories:

- **Security problems**. Corporate information stored on an unsecured personal device is vulnerable to malicious programs designed to steal or damage data. Furthermore, this information could fall into someone else's hands if the device is lost or stolen. For IT Departments, the surge in the number of corporate mobile devices has led to a need for additional security solutions and revised security policies addressing mobile device connections to the local network. Without this the risk of infection for the company's IT infrastructure will rise considerably.
- **Management problems**. Mobile devices that are used within a company, regardless of the type or platform, need support from the company's IT Service. For example, the installation of applications should be controlled by experts in an effort to prevent mobile devices from becoming infected and to protect them against data theft. Ensuring the clear and reliable separation of personal and work-related data on devices is another task that falls on the shoulders of a company's IT professionals. This means that an IT team will need special tools to monitor the appearance of mobile devices on the local network, restrict connections with transient devices, set out policies for access to corporate resources and data, and ensure control over applications, among other things.

Mobile Device Management (MDM), a set of technologies and software solutions, can easily resolve these problems. MDM provides system administrators with the tools they need to manage all of the mobile devices used within a company, regardless of what type of device, or the operating system they run. There are several MDM solutions available on the market today, including a Kaspersky Lab product.

Kaspersky MDM capabilities

By combining two interconnected programs (Kaspersky Mobile Device Management and Kaspersky Endpoint Security 10 for Mobile Devices), Kaspersky Security for Mobile provides a rich set of instruments to protect and manage corporate mobile devices. The first is an add-on program for the tried and trusted Kaspersky Security Center. This facilitates the centralized control of a company's IT security, while the Mobile Device Management software helps manage corporate mobile devices, as well as personal smartphones and tablets, within a company's local network.

Mobile Device Management installs Kaspersky Endpoint Security 10 for Mobile Devices on each smartphone and tablet. This application is another integral part of Kaspersky's Mobile Device Management solution. It serves as the primary security solution and includes antivirus technologies, tools for filtering incoming calls and text messages, data encryption, a jailbreak detection function, and more. The application's precise features will depend on the type of device and its operating system.

A special agent within Kaspersky Endpoint Security 10 for Mobile Devices sets up a connection between mobile devices and Kaspersky MDM, allowing a sys-admin to remotely manage security tools. In particular, an IT professional will be able to update security policies, change device settings, remove corporate data, etc., and most of these actions can be performed without the user even noticing. For example, if a company's IT Department is updating its VPN network settings, Kaspersky MDM can remotely upload all new data to mobile devices. And when an employee needs to connect to the VPN, the phone or tablet will already be able to function fully without having to contact tech support. Immediately after the initial customization, a mobile device and the data stored on it will be fully secured by Kaspersky Lab technologies.

One of the most useful features of Kaspersky Security for Mobile is the segregation of corporate and personal data stored on a mobile device. This makes it easier to encrypt data and ensure that business and pleasure do not mix on a smartphone or tablet. It also lets sys-admins prevent the leakage of corporate data should a mobile device be lost or stolen, or if an employee leaves the company. For example, by using remote access tools, a system administrator can delete a device's profile containing data on the MDM server, along with all of the data, settings, and applications associated with that profile. If there is no need to delete a profile, it can be retained and Kaspersky MDM can be used to remove specific data and corporate applications. For example, if a device continues to be used within the company, this approach will save the administrator from having to create a new profile. Both approaches provide reliable removal of confidential data without coming into any contact with a user's personal information, such as photographs, music, applications, and other data. However, in an extreme or emergency situation, Kaspersky MDM can be used to delete all data and roll a device back to factory settings.

Platform and protocol support

One of the most critical features of Kaspersky MDM is its support for two key solutions used to manage mobile devices: the Apple MDM server, and Exchange ActiveSync (EAS) protocol, which is used to run MDM on the Microsoft Exchange Server. Furthermore, the product also supports built-in MDM solutions, such as Sybase Afaria. These all combine to provide maximum coverage of the mobile platforms available on the market. It also makes integrating Kaspersky MDM into a company's existing IT infrastructure easy, even if it is already using an MDM solution from another developer and has the corresponding security policies in place.

The Apple MDM Server

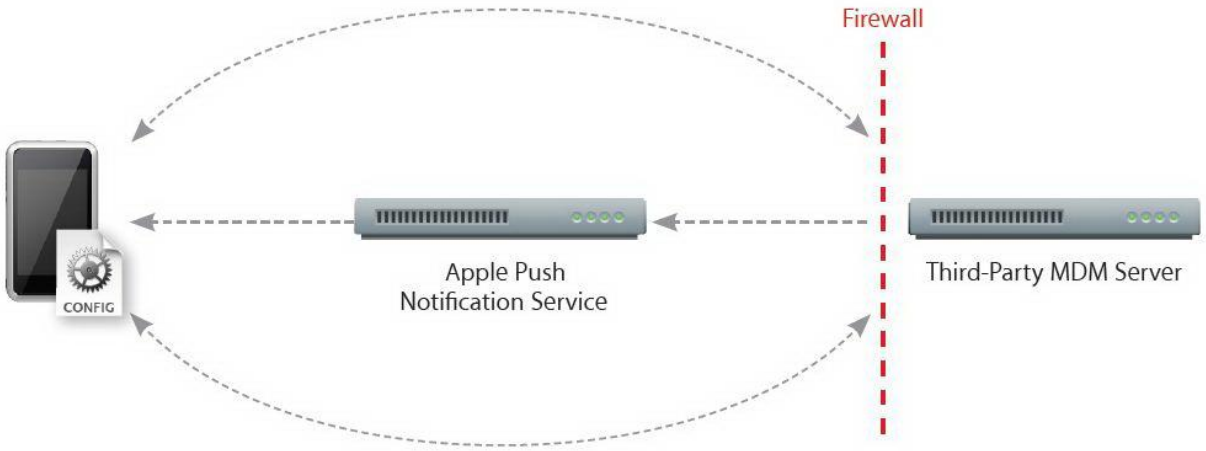
When iOS 4.0 was officially released, Apple offered third-party developers tools for developing MDM solutions making it possible to remotely manage an iPhone or iPad. These tools, known as Apple MDM, have become the alternative protocol to Exchange ActiveSync, which does not fully support Apple devices.

Kaspersky MDM actively incorporates Apple technologies, including those running in the iOS operating system, such as:

- iOS user profiles
- Remote OTA (over-the-air) update and customization uploads
- Apple Push Notification Service.

All of these tools allow a company's IT Department to manage iPhones and iPads connected to the corporate network and remotely send devices customization updates for the operating system while ensuring compliance with the company's security policies, and even remotely block a device and delete confidential data from its memory.

The Apple MDM server installation package is included with Kaspersky Security Center and can be extracted using KSC tools. Devices are set up on the MDM server by downloading a special profile to the device containing all of the requisite security settings. After the profile is installed, the device is able to receive notifications from the Apple Push Notification Service. Each time a push notification is received, the device establishes a direct secure SSL connection with the MDM server, and the server will request information about the device or send it new commands. Once all of the commands have been executed, the server ends the connection until the next push notification is sent.



This is how the basic layout of the communication flow looks between a device and the MDM server:

- **Third-Party MDM Server** – Kaspersky Lab's MDM solution facilitates push notifications and device management commands;
- **Apple Push Notification Service** – Apple's service, which is responsible for transferring push notifications coming from Kaspersky MDM and being sent to a mobile device;
- **Mobile device** – a smartphone or tablet running iOS with an installed MDM profile.

Thanks to close cooperation with Apple technologies, Kaspersky Lab's product fully covers all of its corporate clients' needs when it comes to managing iOS mobile devices.

Exchange ActiveSync protocol

The Exchange ActiveSync (EAS) protocol helps company employees gain access to data (email, contacts, tasks, etc.) stored on the Microsoft Exchange server, in addition to working with them autonomously. Kaspersky MDM uses the EAS protocol to work with mobile devices running on Android, BlackBerry, Symbian, Windows Mobile, and Windows Phone. The functions available to sys-admins through Kaspersky Lab's solution to some extent depend on the particular mobile device and its operating system.

In order to manage mobile devices on a local network via EAS, the company must already use the Microsoft Exchange server for email inboxes and employee mobile devices. As with Apple MDM, a profile downloaded to the device is used as a control tool, and its settings set out the level of security for the smartphone or tablet. The profile is linked to a specific email inbox which, in turn, is linked to the mobile device. If an employee works with more than one email inbox with different MDM policies, then the device will be assigned a profile with more stringent settings. An unlimited amount of profiles can be created within one Microsoft Exchange server, but one of them must be specified as the default, and that profile will automatically be assigned to new Microsoft Exchange inboxes.

Benefits

Kaspersky Mobile Device Management features many advantages:

- Securing corporate smartphones and tablets in addition to the protection already in place for company workstations together with Kaspersky Endpoint Security 10 for Mobile Devices.

- Support for all modern operating systems guarantees that every mobile device — both corporate and personal — will have reliable protection.
- Separation of work-related and personal information stored on devices — this ensures that company data will be safeguarded, without interfering in the private lives of mobile device owners.
- A standard control panel for centralized security management will provide administrators with information about all mobile devices connected to the local corporate network, their users, and their operations. The control panel makes it easy to remotely customize settings for each device individually, or settings for a group of devices.
- The product was developed with SMEs in mind. It is easy to install and does not require additional IT staff to facilitate the management of mobile device security.