IKARUS mobile.security for MDM Manual

IKARUS Security Software GmbH
Blechturmgasse 11
1050 Vienna
Austria

© IKARUS Security Software GmbH

www.ikarussecurity.com

Contents

List of figures

List of tables

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

1 Introduction

This is the manual for IKARUS mobile.security for MDM, the Android anti-virus and web security solution developed by IKARUS Security Software for Mobile Device Management (MDM) systems. The audience of this document are IT administrators of companies who will use and embed IKARUS mobile.security for MDM either in their own MDM system or in an MDM system by a third-party vendor.

The IKARUS mobile.security version available on Google Play and on the IKARUS web site is for private end consumers. Unlike the MDM version described in this manual, the end-consumer version is not specialised for business use and differs from it in the following aspects:

- In order to activate full-version features after a free 30-day trial, a purchase via Google or using an IKARUS activation code is necessary. In the MDM version, a signed license file is pushed on the device. The expiration date of the license is contractually agreed upon previously.
- Features which:
  - ✓ are more interesting for private use,
  - ✓ require much user interaction to configure correctly,
  - ✓ or interfere with features already provided by an MDM system,

have been removed from the MDM version. This includes remote control via messages (lock device, localise, reset, alarm), the text message blacklist, SIM-change detection and USSD protection.

- The user interface is much simpler in the MDM version.
- In the MDM version, the user cannot modify any settings; the MDM administrator instead transfers a signed configuration file on the device which the app then automatically detects and processes.
- There is no system for automated upgrades in the MDM version. This is unlike the integration offered by the Android operating system for Google Play apps. The MDM software must push new versions of the app on the devices after IKARUS has provided them.
- This usually happens a few times a year for various improvements and optimisations. It has nothing to do with the database updates offered several times a day; those will work as expected in the MDM version.
- The MDM application package is not available for download on Google Play.
- The MDM version adds custom blacklisting and whitelisting for URL filtering.
- The MDM version adds the "Threat Statistics" feature.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

Therefore, IKARUS mobile.security and IKARUS mobile.security for MDM are really two different products; while they share some of the same basic components, they achieve different goals, have a different user base and are handled in a different way.[1]

Section 2 discusses licensing possibilities. Section 3 explains the features of the app (virus scanning, URL filtering and threat statistics). Section 4 then goes on to explain strategies to apply licenses and app configurations to your end users' devices and documents a helper tool provided by IKARUS to ease that task.

```
----- BEGIN IKARUS SOFTWARE LICENSE -----
product IMSMDM
serialnumber HF2517216
owner Your Company
describtion IKARUS mobile.security MDM
startdate 2013-11-20
enddate 2014-11-30
features scanonaccessapp ; scanondemandapp ; scanondemandfull
----- SIGNATURE -----
PLGdDZIzjDhX8ANF28CwW7jAp8LWfZ++2q1xGN6xkHMej2Ac+8gLl l ro fpT /9VpiJQ0
h6VMwjXAD5qVYVnpyO4FV7MdNyofFkXvbw0l6RN4kexMnOmihDTeDslFObfB4xtRuak
uxhZJAsadzeq8lhJnt9wqjkTgOmS+FHEHqC1E=
----- END IKARUS SOFTWARE LICENSE ------
```

Figure 1: An example of a license file

It is a plain-text document with an embedded digital signature. You receive this file from IKARUS when you buy the software and must later deploy it to end-user devices.

1 It is technically possible to run both versions on the same device. Despite of an identical name shown to the outside, they differ in the way they register themselves in the operating system. There is, however, no scenario in which this could be of any practical use.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

2

Licensing

The license for IKARUS mobile.security for MDM is previously agreed upon between IKARUS and the customer in the contract. IKARUS then provides a digitally signed license file, as shown in Figure 1, which states the previously agreed-upon expiration date. The file must be transferred to every end-user device on which the IKARUS app is installed or will be installed. Section 4 explains deployment strategies.

The license not only contains the expiration date but also specifies which features have been bought by you and can thus be activated in the app through the MDM software. The latter is usually not important, because you will have typically bought a license with all features activated. If you think your business may benefit from more granular licensing, please contact the IKARUS sales department. Section 3 explains all available features in detail.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

3

App Features

IKARUS mobile.security for MDM has three ways to aid you in protecting your end user's devices: Virus scanner, URL filter and Threat statistics (interface). Virus scanning, explained in detail in Section 3.2, scans the device for viruses. The URL filter, explained in detail in Section 3.3, blocks the web browser if a dangerous web page is opened. Threat statistics, explained in detail in Section 3.4, means that the app contacts a dedicated server to notify it about virus detections or visits of dangerous web pages.

You will see that the app has a very slim graphical user-interface, shown in Figure 2. As the app is meant to be configured and maintained by MDM administrators, there is little to be done for end users themselves. They can start additional scans and database updates, but cannot otherwise interfere with administrator settings.

3.1 Updates

Both the virus scanner and the URL filter work reliably if they are regularly adapted to the latest threat scenarios. In order to achieve this, IKARUS provides a data base on its web server which is updated several times a day and which the app may download at any time. The database contains virus definitions and URLs which IKARUS has classified as dangerous.[2] The transfer of the data base from the IKARUS web server works with an ordinary Internet connection. The MDM software itself is not involved. Updates can be initiated manually by the end user or automatically by the MDM administrator setting an update interval in the configuration, as explained in Section 4.2. In order to update manually, the end user navigates to the "AntiVirus" area of the app and clicks "Update". Automatic updates, however, usually prove to be more useful in corporate environments. This is done by the MDM software defining an interval by which the app queries the IKARUS server for new data base versions. See Section 4.2.

The latest version of all updatable components are downloaded from the IKARUS server when the app is started for the first time.

2 Sometimes, updates replace not only the data base but also the scan engine and the AntiSPAM engine, which is needed for URL filtering, with new versions. Those two components do not change very often. Expect it to happen only a few times per year.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

Note that the upgrade of the app itself is a different issue altogether! It happens very seldom, and the MDM software must perform it by whatever device-management mechanism is appropriate for it. IKARUS will contact you if a new version of the app is available for customers.

3.2 Virus Scanner

The virus scanner analyses apps installed on the device and any kind of files in the publicly accessible file system (such as the SD card, or files downloaded from web pages). In order to do so, it uses a virus data base, which is always kept up-to-date, and warns the user in the case of a positive result.

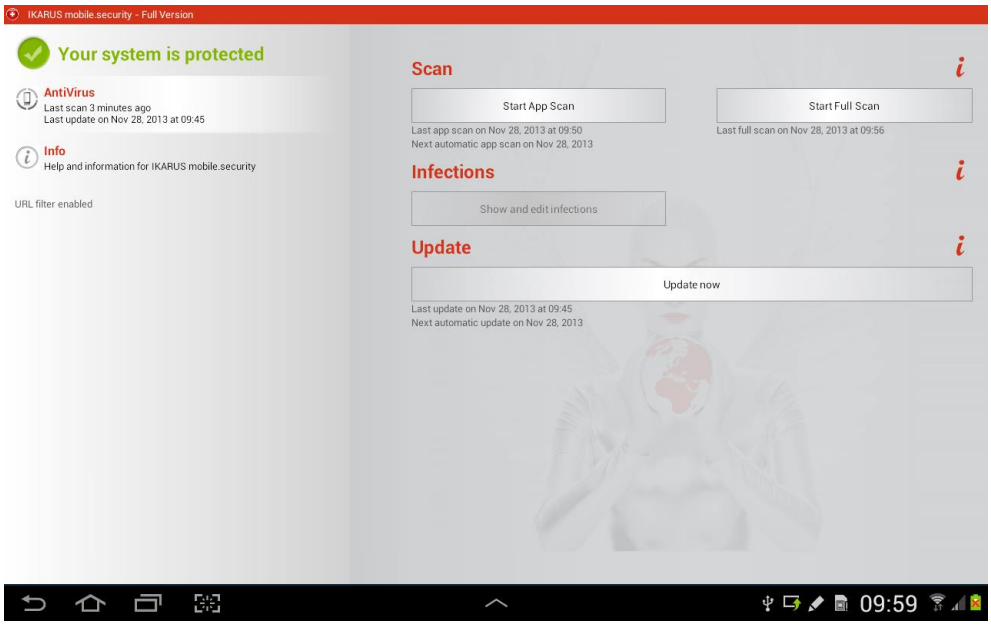

Figure 2: The app's main screen viewed on an Android tablet

It offers little end-user interaction, because it is meant to be configured and maintained by the MDM administrator. Even so, the user can start additional scans and database updates at any time.

The following kinds of scans are supported:

- On-demand scan by the user
  The user navigates to the "AntiVirus" area of the app and clicks "Start app scan" or "Start complete scan". The former scans the apps installed on the device, the latter additionally scans publicly accessible storage (such as the SD card or the integrated storage).
- Automatic on-demand scan defined by the MDM software in certain intervals
  Here, too, you can select the scope of the scan to be either app-only or full.
- On-access scan
  The app scans proactively when an app is installed or upgraded on the device or when a file is placed on public storage (such as copied on the SD card or downloaded with a web browser).

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

When a virus is detected, a full-screen warning as shown in Figure 3 appears and the user is asked whether the infected file should be eliminated. All virus scans are based on the data base and scan engine currently present on the device.

Other options in the case of an infection:

- Ignore
  When the user is aware of the dangers or is absolutely sure that the scan result is wrong, then he or she can define certain apps or files to be whitelisted, so that future scans will ignore them.
- Send file to MDM administrator
  The user can send an infected file via e-mail attachment to an address previously configured by the MDM software in order to ask for a manual analysis, or you can configure the app such that infections are sent to the IKARUS malware-analysis laboratory. See Section 4.2.

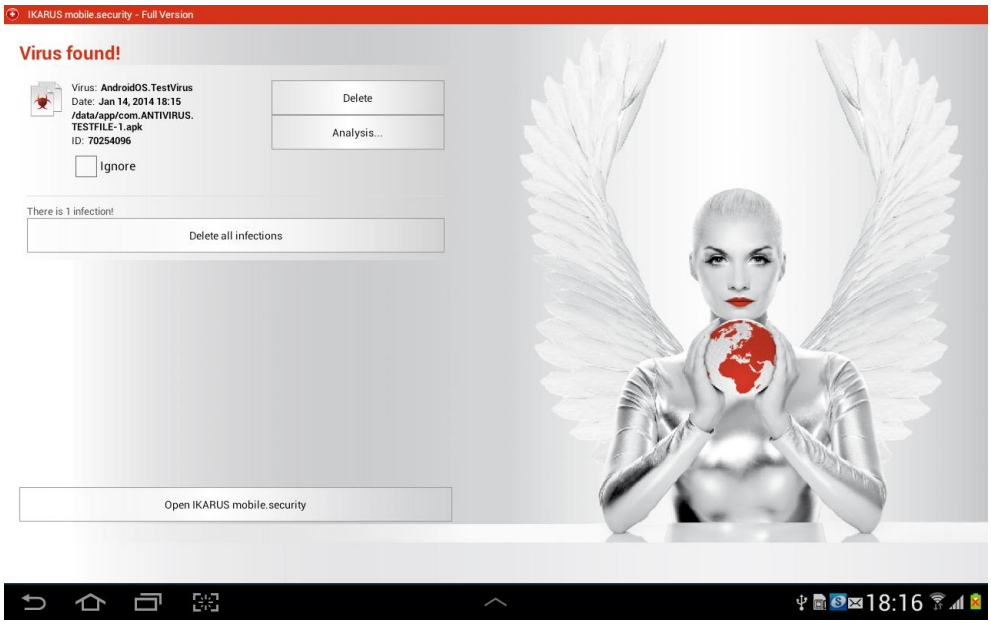

Figure 3: Warning message when virus is found

When a virus is found by the IKARUS app, a full-screen warning message appears and the user can delete the infected file. Other options include temporarily ignoring it and sending it to either the MDM administrator or to the IKARUS malware-analysis laboratory.

The "AntiVirus" area of the app also contains the infection list which shows the user if and which viruses are currently present on the device. This is also where you can unignore files.

On request (see Section 4.2), a service called "Signature Quality Assurance" (SigQA) can be enabled in the background. SigQA is a tool for anonymised processing of virus statistics, used by our malware analysts to improve scan quality. When SigQA is enabled, anonymised data is transferred in the background to an IKARUS server.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

Files or apps may be classified as viruses due to a web URL contained in them. This is mostly the case with adware. If an infection is caused by a contained URL, the offending address is shown in the infection list alongside the file.

3.3 URL Filter

The URL filter is a fully automated web-protection mechanism. The classification of web pages as dangerous is based on a URL basis. The app principally uses the data base and AntiSPAM engine currently present on the device.

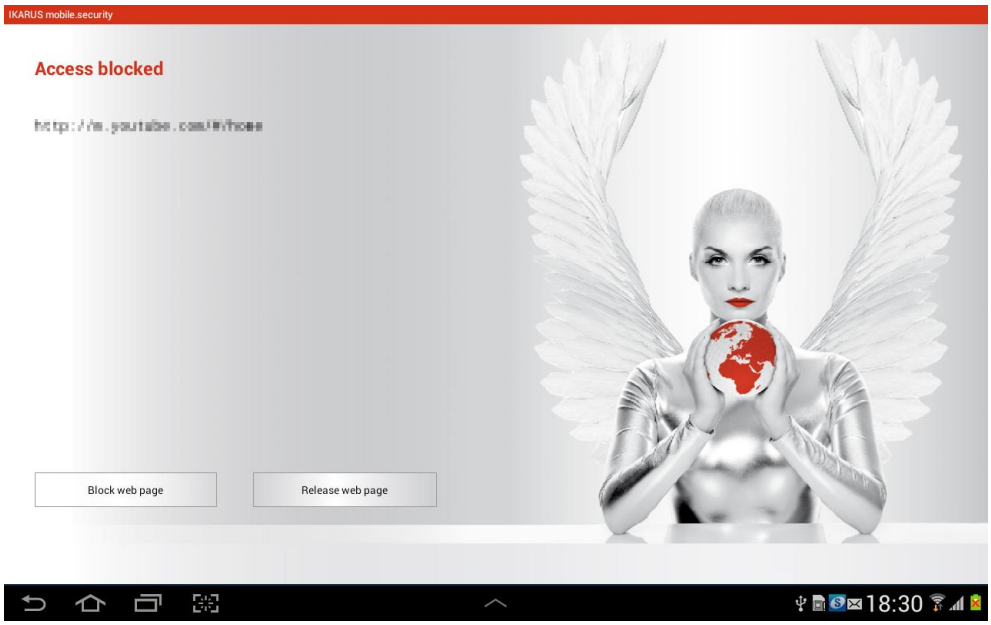

Figure 4: Access blocked – dangerous website detected

The app detects suspicious pages from the IKARUS database or your own custom blacklist when they are to be opened in the web browser. A full-screen warning message is shown in such cases, and the user has the choice of whether to visit the page anyway or block it. If the former is chosen, then the app will remember the choice only until the device is rebooted.

Manually adding URLs or domains (blacklisting) or excluding certain URLs or domains (whitelisting) is also possible; Section 4.2 contains instructions on how you can add those custom entries. For example, you could set your blacklist to "facebook.com;youtube.com" and your custom whitelist to "example.org;example.com;example.net".

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

The whitelist applies to your own blacklist entries as well as for the IKARUS database. So if your blacklist was "facebook.com;youtube.com" and your whitelist was "example.org;example.com;example.net;youtube.com", then youtube.com would not be considered by the URL filter.

If a URL classified as dangerous is to be opened in the browser, a warning message is displayed on the screen and the user is asked whether the page should be visited anyway or continued to be blocked. Figure 4 shows what users see on their screens if this happens. Temporarily unblocking a page is not permanent but will be reset at the next reboot of the device.

The URL filter works with the Android stock browser and Google Chrome, BUT not with alternative browsers like Firefox or Opera.

3.4 Threat Statistics

Threat statistics means that the app contacts a dedicated server in the case of events such as virus detections or visits of dangerous web pages. A business customer can easily write a server application to retrieve that data and generate statistics from it on a device-by-device basis.

The app features an interface which a dedicated server application can utilise to create statistics of threats from infections and dangerous URLs. This feature works with an HTTP connection to a server address set in the configuration; see Section 4.2.

Certain events occurring in the app make it send an HTTP request with certain data, including device identification (IMEI). Using this mechanism, it is, for instance, possible to detect which viruses appeared on which devices and which URLs were detected. If the server is not accessible at the time of the event (which will often be the case in the mobile context), the data is cached locally, and a new sending attempt is made every day.

Recognised infection events:

- virus found,
- virus removed,
- virus ignored,
- virus unignored.

Recognised URL-filter events:

- dangerous URL found,
- dangerous URL blocked,
- dangerous URL not blocked.

Different server URLs can be specified for infection events and URL-filter events.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

In the URL for infection events, the following parameters can be specified, each preceded by a dollar sign:

- action (= found, removed, ignored or unignored)
- imei
- filename
- signatureName
- signatureId
- packageName
- url (if a file is classified as virus due to a URL contained in it)
- when

For example, the configuration may set the request address template to the following value:

```
http://www.example.com/notify?event=$action&filename=$filename&device=$imei
```

Now suppose a virus called „malicious file.apk“ was detected on a device with IMEI 12345. The resulting request URL would be as follows:

```
http://www.example.com/notify?event=found&filename=malicious\%20file.apk&
device=12345
```

URL-filter events work the same way but offer the following parameters:

- action (=hit, blocked or not blocked)
- imei
- url
- when

In order to utilise this feature, the customer must implement server-side support. IKARUS only provides the client side.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

4

Deployment

The deployment process for IKARUS mobile.security for MDM involves two installable APK packages:

- IKARUS mobile.security.apk

the actual, working main app. This one is provided directly by IKARUS.

- MDMHelper.apk

a helper app which equips the actual app with license and configuration information. This one is created by you, using an IKARUS tool which will be explained in detail in the following sections.

Both apps must be deployed to end-user devices just like any other app with your MDM. You must make sure that end users not only install but also run the apps once after installation. The order in which the apps are installed and started does not matter.

Note that the main app will automatically start on subsequent device reboots, but it must be launched at least once by the user first, as is the case with all pro-active Android apps.

The helper app contains a license and a configuration. Consequently, every license and configuration combination or change constitutes a different helper app. IKARUS therefore provides a tool to create helper apps from scratch.

That tool is included in the package you received when you obtained IKARUS mobile.security for MDM. It is an executable command-line Java application tool called "create-ikarus-mdmhelper.jar", and it will create a fully functional, installable and runnable helper-app APK with license and configuration included, given three things:

- A certificate for the helper-app with password and alias, in the form of a file. All of this can be created in a single step with the Android SDK Tools. You can create it once and reuse it subsequently. Alternatively, IKARUS can provide you with a certificate. The name of the file typically ends with ".keystore". Section 4.1 explains this step in more detail.
- A valid license file (previously signed by IKARUS and received from you when you obtained the software from IKARUS). The name of the file typically ends with ".ikkey". Review Section 2 for more information about the license file.
- A configuration file written by you, containing your custom settings. The file will be automatically signed later on by the tool. The name of the file typically ends with ".config". Section 4.2 documents configuration options.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

```
automaticScansEnabled=true
automaticScansInterval=50000000
automaticScansMethodFull=false
automaticUpdatesEnabled=true
automaticUpdatesInterval=5000000
appProtectionActivated=true
sdCardProtectionActivated=true
updateOnlyWifi=true
sigqaActive=false
webFilteringEnabled=true
customUrlBlacklist=facebook.com;youtube.com
customUrlWhitelist=example.org;example.com;example.net
sendInfectionRecipient=mymail@myorganisation.com
infectionProtocolUrl=http://www.myorganisation.com/notifyVirus?event=$action&filename=
$filename&device=$imei
urlFilterProtocolUrl=http://www.myorganisation.com/notifyUrl?event=$action&device=
$imei&time=&when
```

Figure 5: An example of a configuration file

The MDM administrator writes such a file, using the available options shown in Table 1 in the parameter=value format. The file is digitally signed and embedded into a helper app with a special deployment tool provided by IKARUS.

The following sections describe the steps involved in creating and using the helper app.

4.1 Creating Your Helper-App Key

Official Android documentation at http://developer.android.com/tools/publishing/app-signing.html contains an extensive guide on signing apps. Signing is important because for security reasons, an Android device will normally refuse to install or run unsigned apps.

You can either create a certificate with the private key yourself or request one from IKARUS. The former solution allows you to better secure your key, the latter may be more comfortable for your business.

Creating the certificate yourself will typically involve a command-line call such as:

```
keytool –genkey –v –keystore MDMHelper.keystore –alias MDMHelper-keyalg RSA –
keysize 2048 –validity 10000
```

When prompted, choose a password and leave all other data empty.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

Consult the Android documentation for more details. In any case, you will later need the file ("MDMHelper.keystore", taking the example from above), the password and the alias.

4.2 Configuration

The end-user cannot modify any settings on the device; each and every configuration of the app is made exclusively by the MDM administrator. When administrators want to create a set of configuration options, they create a plain-text file as shown in Figure 5.

Table 1 contains a complete list of all supported parameters in the configuration file. Every parameter has a default value, which is applied by the app if the configuration file does not contain it. Furthermore, every option has a type. A “Boolean” type means that something can be enabled or disabled, a “Long” type means that something is a (possibly very large) integer number and a “String” type means that something is text. For each value specified in the configuration file, the app will check if it matches the parameter’s type.

String values must not be enclosed in apostrophes. For example, in order to set sendInfectionRecipient to a certain e-mail address, you need the following line in the configuration file:

```
sendInfectionRecipient=email@example.com
```

It would be an error to use the following line instead:

```
sendInfectionRecipient="email@example.com"
```

Millisecond options for automatic scans and updates provide administrators with a very fine-grained control mechanism. For example, 86400000 means “daily”, because 1000 milliseconds = 1 second, 60 seconds = 1 minute, 60 minutes = 1 hour, 24 hours = 1 day, thus 1000 × 60 × 60 × 24 = 86400000.

The user can see (but not modify) the configuration in the “Info” area of the app. Administrators, however, can use this information to verify that their configuration was applied correctly.

4.3 Publishing Your Helper App

The tool to create your helper app is a Java command-line application called “create-ikarus-mdmhelper.jar”.

In its basic form, relying on default values and default filenames (“license.ikkey” for the license file and “ikarus.config” for the configuration file), you run it like this:

```
java -jar create-ikarus-mdmhelper.jar -storepass YourKeyStorePassword
```

“YourKeyStorePassword” is the password you chose previously when creating the certificate.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

The tool will create an app file called “MDMHelper.apk”. This app must be distributed by the MDM administrator, and end users must eventually run the app.

When the app starts, all it does is placing the license and the configuration on the device such that the actual app will automatically pick them up.[3]

3 The technical implementation is such that a license file and a configuration file are placed at public file storage of the end-user device. The IKARUS app picks them up from there. Those files could be put there in any way which is technically possible. Your MDM may even support file transfer directly. Further possibilities include e-mailing the files to end users or having them downloading them to the right place. However, these approaches would likely turn out to be too clumsy or inappropriate for your business. The helper-app approach hides technical complexity and is less error-prone.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

Name	Description	Type	Default
automaticScansEnabled	Scheduled automatic scans enabled?	Boolean	false
automaticScansInterval	Frequency of automatic scans in milliseconds	Long	86400000
automaticScansMethodFull	Scheduled automatic scans are full scans?	Boolean	false
automaticUpdatesEnabled	Scheduled automatic updates enabled?	Boolean	true
automaticUpdatesInterval	Frequency of automatic updates in milliseconds	Long	43200000
appProtectionActivated	Automatic app scans enabled?	Boolean	true
sdCardProtectionActivated	Automatic scans for external storage enabled?	Boolean	true
updateOnlyWifi	Updates only via Wi-Fi?	Boolean	false
sigqaActive	SigQA enabled?	Boolean	true
webFilteringEnabled	URL filter enabled?	Boolean	false
customUrlBlacklist	Custom URL blacklist (separated by semicolons)	String	
customUrlWhitelist	URL whitelist (separated by semicolons)	String	
sendInfectionRecipient	Custom e-mail address to send infections to	String	
infectionProtocolUrl	URL for notifications upon infection events	String	
urlFilterProtocolUrl	URL for notifications upon URL-filter events	String	

Table 1: Available Configuration possibilities.

All available configuration options, along with default values and types. These can be used in the plain-text configuration file written by the MDM administrator. The default value is applied by the app if the option does not appear in the configuration file. As far as types are concerned, "Boolean" means that something can be enabled or disabled, "Long" means that some- thing is a (possibly very large) integer number and "String" means that something is text. Figure 5 is an example of a configuration file using some of these options.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

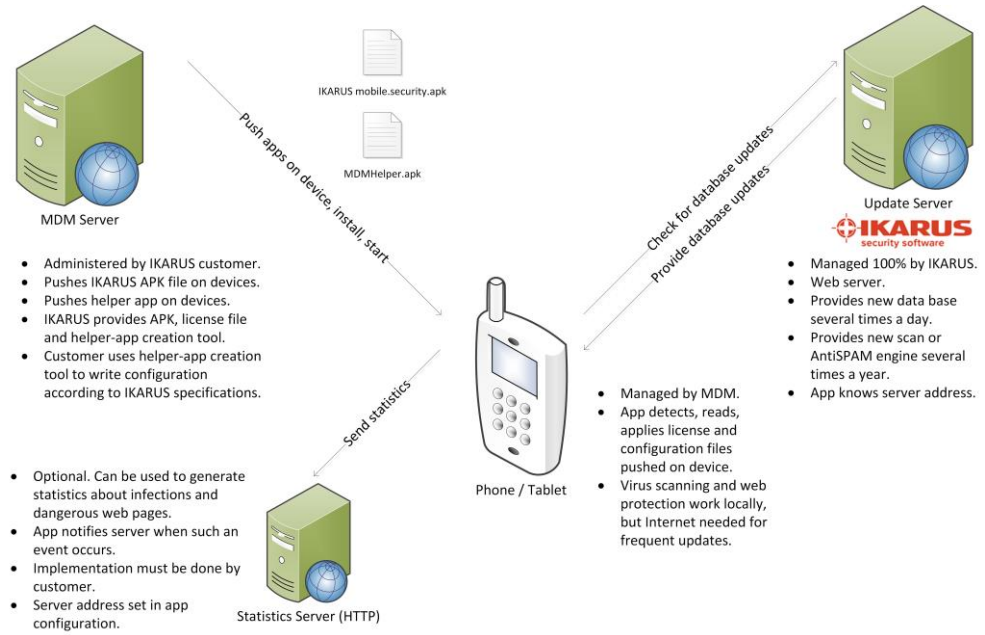

Figure 6: Functionality IKARUS mobile.security for MDM

Servers interacting with each other and with the Android device make up the entire protection architecture. The MDM server pushes the IKARUS app and the helper app on the end- user device. From there, the IKARUS app regularly accesses the IKARUS update server for database updates and optionally sends threat statistics to yet another custom server.

At this point, the helper app may be uninstalled again, although that is not necessary. Leaving the helper app on the device and allowing users to rerun it does not do any harm.

Figure 6 depicts the entire MDM system with all major components: the MDM server pushing the two apps on the end-user device, the IKARUS update server providing database updates to the end-user device, the threat-statistics server maintaining statistics received from the end-user device, and the end-user device itself in the centre of the information flow.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Vienna/Austria | Phone.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Company register: FN 64708i | Venue Vienna | VAT-Nr.: ATU15191405

5 Contact

IKARUS Security Software GmbH

Blechturmgasse 11
1050 Vienna
Austria

Phone: +43 (0) 1 58995-0
Fax: +43 (0) 1 58995-100

office@ikarus.at
www.ikarussecurity.com

IKARUS Security Software Support Contact

Phone: +43 (0) 1 58995-400
Support times: Mo-Do: 8.00 – 18.00 (MEZ)
Fr: 8.00 – 15.00 (MEZ)
E-Mail: support@ikarus.at

IKARUS Security Software Sales Contact

Phone: +43 (0) 1 58995-500
E-Mail: sales@ikarus.at