IKARUS mobile.management

Activation der IKARUS mobile.security

Release date: 16.11.2022

Version: 1.1

IKARUS mobile.security application is an anti-virus and anti-malware client for devices running the Android operating system.

This document describes the rollout and activation process for the IKARUS mobile.security (IMS) app via IKARUS mobile.management (IMM).

For the optimal use of this document, you should be aware of the MDM basics as well as the MDM menu navigation.

Preparations

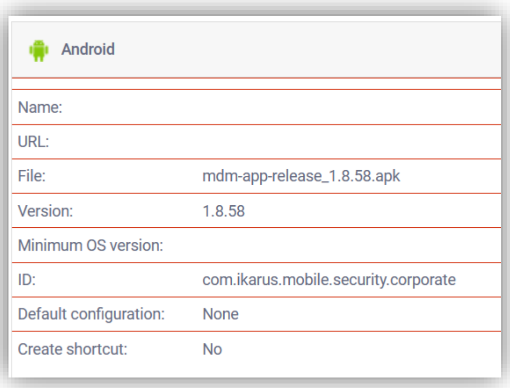
The following preparations must be completed before the IMS application can be enrolled.

1. Application

1. Add a new application in you MDM system.
2. Upload the latest version of the IMS application and wait until the version number and application id are shown.
3. Save the application package.

The current version number is: 1.8.58

You will find the latest IMS application here: https://mdm.ikarus.at/client/



Android

Name:	
URL:	
File:	mdm-app-release_1.8.58.apk
Version:	1.8.58
Minimum OS version:	
ID:	com.ikarus.mobile.security.corporate
Default configuration:	None
Create shortcut:	No

2. Configuration

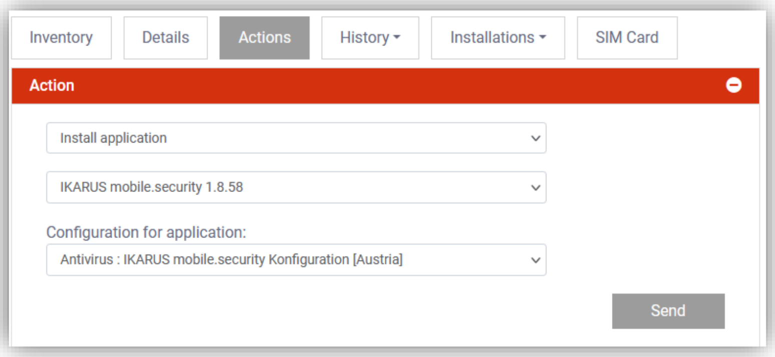
1. Add a new configuration with configuration type „Antivirus“.
2. Define the parameters for your configuration. – details can be found **here**.
3. Save the configuration template.

Rollout

Please perform the following steps to enroll the IMS application.

1. Single device – action

1. Navigate to the desired device in Organization > Users and devices > device.
2. Open the action menu for the device.
3. From the dropdown menu select the action **install application**.
4. Select the IMS application package.
5. Select the configuration for application you created previously.
6. Press the send button.



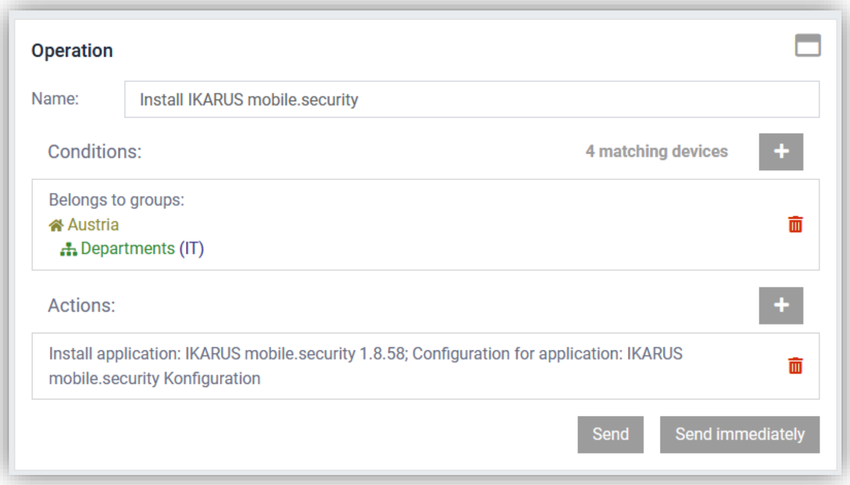
Install application

IKARUS mobile.security 1.8.58

Configuration for application: Antivirus : IKARUS mobile.security Konfiguration [Austria]

2. Several devices – operation

1. Navigate to the menu Operations > Operations.
2. Add a new operation.
3. Set the conditions to define the devices that should be selected for the rollout.
4. Select the actions install applications with the according IMS package.
5. Select the configuration for application with the previously created configuration.
6. Save the operation.
7. Press the button send to apply the actions or the button send immediately to apply the action and send a forced connection.



Name: Install IKARUS mobile.security

Conditions: 4 matching devices

Belongs to groups:
Austria
Departments (IT)

Actions:

Install application: IKARUS mobile.security 1.8.58; Configuration for application: IKARUS mobile.security Konfiguration

Important notes

Licensing

The licensing of the IKARUS mobile.security application is done via a combination of the components IMS client and a valid configuration. If both components are present on the device and the device is managed via a licensed IMM system, a license is issued for the device via the license server. A license file or activation code is no longer required.

Scope of functions

The functionality of the IMS application depends on several device-specific factors. Depending on the device used and the version of the operating system, special features may not be available. For some functions, it might be necessary for the device user to manually assign corresponding permissions for the application in the device's settings

Installation and activation

Installation and activation may vary depending on the MDM activation method, the device itself, and the version of the operating system. For example, if silent installation is not supported, it is necessary for the device user to manually confirm this installation and grant special permissions.

Appendix

Parameter	Explanation	Recommended value
Automatic scanning	Defines, if automatic scans should be performed on the device.	yes
Automatic scan interval	Defines, how often a scan should be performed	Daily or twice a day
Full scan	Defines, if full scans should be performed or quick scan only.	yes
Automatic updates	Defines, if database updates should be performed automatically	yes
Automatic update interval	Defines, how often database updates should be performed.	Daily or twice a day
Automatic application scans	Defines, if applications should be scanned.	yes
Automatic external storage scan	Defines, if the external storage should be scanned	yes
Updates only via WLAN	Defines, if database updates should be performed via WLAN only	no
SigQA	Enables an additional reporting feature, which sends new but unknown signatures to IKARUS	yes
URL filter	Defines, if the web filter should be activated. This function is supported for specific browsers only (Chrome and native Samsung Browser)	Depends on use case
Custom URL blacklist	Only visible, if URL filter is active. Defines a list of prohibited websites.	Depends on use case
Custom URL whitelist	Only visible, if URL filter is active. Defines a list of allowed websites.	Depends on use case
Enable web filter buttons	Only visible, if URL filter is active. If activated, this feature shows buttons when a blacklisted. These buttons allow to skip the blacklist warning.	Depends on use case
Show virus infection notifications	Defines, if a user should be informed about virus findings on the device or not.	yes
Enable security advisor	Defines, if the security advisor should be activated.	Depends on use case.