



mobile.management

Quick Start Guide

Table of Contents

1	General	4
1.1	Scope.....	4
2	Navigation	5
2.1.1	Breadcrumb	5
2.2	UI layout.....	5
2.3	Basic navigation	6
2.3.1	Command navigation.....	6
2.3.2	Home hyperlink.....	6
2.4	Menu Items	6
2.5	Coloured status indicators.....	7
2.6	General error messages	7
2.7	Tenancy and Language selection, logout	7
2.8	Display Tooltip.....	8
2.9	Greyed (read-only) items.....	8
3	Administrators, Users and Groups	9
3.1.1	Initial login.....	9
3.1.2	Create additional administrator accounts.....	10
3.2	Creating Hierarchies and Groups	10
3.2.1	Creating a simple group hierarchy	11
3.3	Adding a new user	11
3.3.1	Deleting a user	12
3.4	Adding multiple users via CSV file import.....	12
4	Adding a basic Android device	13
4.1.1	Basic Android SIM device SMS enrollment.....	13
4.1.2	Basic Android Wi-Fi device email enrollment.....	14
5	Adding an iOS device	16
5.1.1	Adding an iOS SIM device	16
6	Adding Android Enterprise functionality	18
6.1	Requirements	18
6.2	Preparation.....	18
6.2.1	Global tenant check.....	18
6.2.2	Tenant check.....	18
6.3	Enroll enterprise	19
6.4	Device rollout.....	20
6.5	Official Device List	23
7	Managed Google Play (custom) store layout editor	24
7.1	Using the managed Google Play store (custom) layout editor.....	25
7.2	Work profile – Device view.....	26
7.2.1	Google Store (custom) layout editor - walkthrough.....	27
7.2.2	Rename Page 1 (default) to Homepage	27
7.2.3	Example 1.....	28
7.3	Example 2.....	30

Table of Figures

Figure 1 IKARUS mobile.management server 5.30.00 Global navigation overview.....	5
Figure 2 Error message format	7
Figure 3 Tooltip - field "call out on" mouse hover	8
Figure 4 Hierarchy & Groups command summary.....	10
Figure 5 URL link opened to the profile process.	16
Figure 6 Device Play Store (work profile) Works account view	24
Figure 7 Default (as shipped)	24
Figure 8 Google Play Store (custom) layout editor tab	24
Figure 9 IKARUS mobile.management Server and Device appearance	25
Figure 10 Managed Google Work Store layout editor - Page 1 edit	27
Figure 11 Managed Google Work Store layout editor - Page 1 renamed.....	27
Figure 12 Managed Google Work Store layout editor - Add app	29

1 General

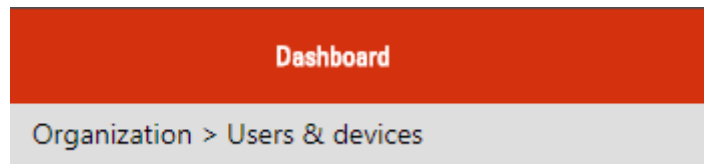
1.1 Scope

The Quick Start Guide is the collection of all published Quick Start Segments, contained within one convenient document, allowing the user speedy access to information that should assist in their productivity with the IKARUS mobile.management server in the shortest possible time.

2 Navigation

2.1.1 Breadcrumb

A breadcrumb is displayed in the top left hand corner of the UI, allowing users to identify their current location within the IKARUS mobile.management system.



The breadcrumb is only an indicator and is not an active link.

2.2 UI layout

IKARUS mobile.management server navigation is achieved by selecting a heading item from the horizontal main menu navigation bar (Dashboard, Organization, Infrastructure, Operations, Reports and (System) Settings), located at the top of the IKARUS mobile.management server UI, which when selected, will reveal vertical drop-down navigation sub-menu items that are associated with the selected main menu heading.

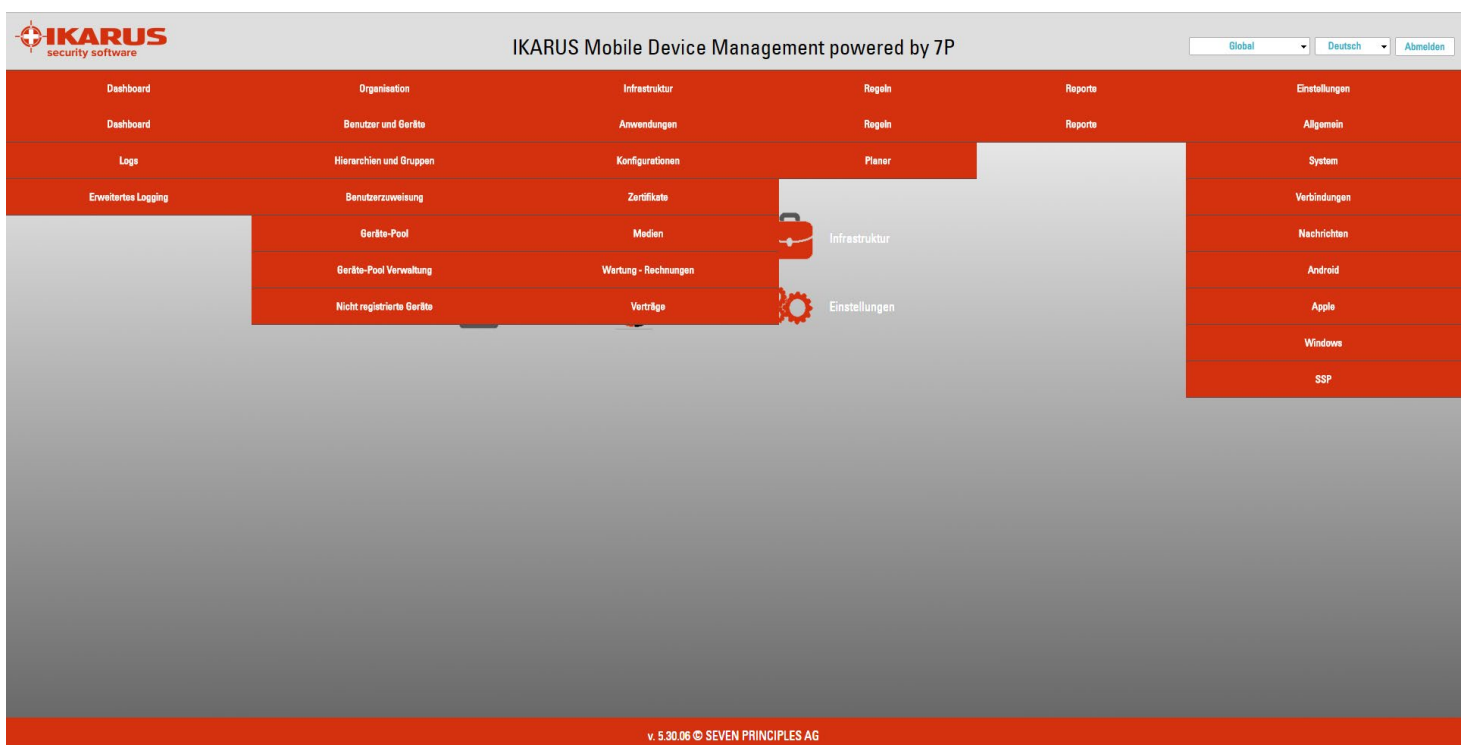


Figure 1 IKARUS mobile.management server 5.30.00 Global navigation overview

Selecting a sub menu item such as Dashboard for example will open the Dashboard control panel window

2.3 Basic navigation

Navigation through the various header menu, sub menus, and panels is short formed in this document in the following way:

Navigate to **System settings > Settings > Base > Tenants** will instruct the administrator how to locate the “Tenants” configuration panel within the IKARUS mobile.management server.

2.3.1 Command navigation

Command navigation consists of a command tagged onto the navigational direction: Select the **Organization > Hierarchies & groups > Add a new hierarchy** will instruct the administrator how to locate the “Add a new hierarchy” command within the IKARUS mobile.management server.

2.3.2 Home hyperlink

A hyperlink ([^Home](#)) is inserted into the bottom right-hand side of the footer which when clicked will return the reader to the beginning of the document and is only active in PDF format.

2.4 Menu Items

The greater than sign (>) with spaces before and after the sign, separates items in the menu. For example, **Operations > Operations > Is roaming > Drop-down selection (Yes / No)** indicates that you first choose “Operations” from the main tabs, then “Operations” from the left-hand menu options, followed by the selection of an operation name, then the condition to be applied.

2.5 Coloured status indicators

Coloured status indicators are designed to assist the administrator by highlighting (through colour) selective performance indicators, whether a status or metric is either within or outside the desired range.

Security	
MDM Client password	Password is not set <input type="button" value="Set new password"/>
MDM Security code	Not permitted
Jailbroken/Rooted	No
Device Encryption	Block+File
Compliant	Yes
Supervised	No
Activation lock	Yes
Locator service (Find My iPhone)	Yes
Do not disturb	No

At present, three colour indicators exist on the IKARUS mobile.management server: Green – All OK, Yellow – attention required and Red – Alert!

2.6 General error messages

Error messages in general are designed to inform the administrator why a specific function fails to execute; if there is a data conflict, type mismatch, or desired parameter is already in use.

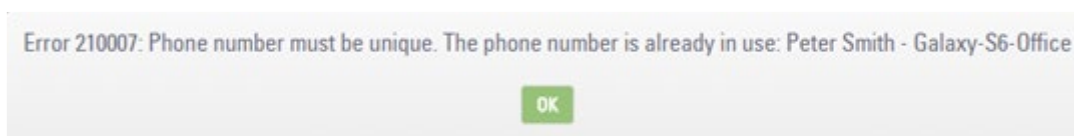
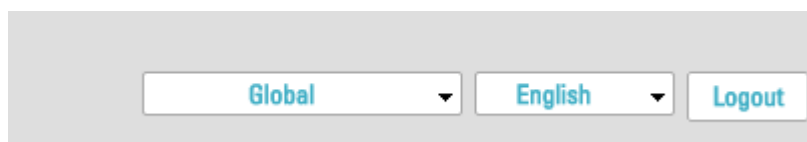


Figure 2 Error message format

Error messages where possible contain exact information. In the case of the above data conflict, the IKARUS mobile.management server displays the reason for the error and supplies further information, notably User, Tenant and device name.

2.7 Tenancy and Language selection, logout

The Tenancy and language selection drop-down lists are located in the top right hand corner of the IKARUS mobile.management server GUI.



Selecting the Logout action button, will log the user out.

2.8 Display Tooltip

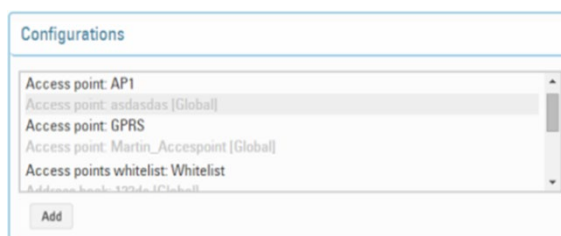
An information pop up will be revealed, when certain condensed information fields are hovered over with the mouse, which will allow the administrator to copy and paste the full information field into, for example, a Notepad document.

Hardware	
Serial number	C32JXQ6
Firmware	12H321
User agent	iPhone, MD297KN, 8.4.1 12H321
Product ID	iPhone5,2
IMEI	01341 <small>Model: iPhone5 (GSM+CDMA)</small>
MAC	f4:f1:5a:01:d4 f4:f1:5a:01:d4
Udid	e45ad6...84d
Battery	67 % <small>e45ad60a3631800e7238f130037b4984d</small>
	Memory available
Flash	96% (12.0 GB/12.6 GB)

Figure 3 Tooltip - field "call out on" mouse hover

2.9 Greyed (read-only) items

Two discrete colours are used to designate write enabled (editable) and read-only (non-editable) commands and information throughout the entire IKARUS mobile.management server



- Read only configuration elements are usually configured (and protected) by the Super Administrators security credentials.
- Read-only information can also include information retrieved from a mobile device and is read-only by default.
- Read-only information can also include absolute values, information, and totals; the information retrieved and displayed in a report for example.



Any Configuration template, Application, or parameter that has the **[Global]** suffix is only editable by a Super Administrator. Any Configuration template, Admin role or parameter will have the originating/creating tenancy name clearly displayed as a suffix in the Global tenant's view. e.g. Access Point **[Documentation]**

3 Administrators, Users and Groups

The IKARUS mobile.management server will come preconfigured with either Global Super Administrator accounts, or a defined tenancy, with Tenant administration accounts.

Typically you receive notification of the URL for your IKARUS mobile.management server tenancy, the tenancy administrator username and password.

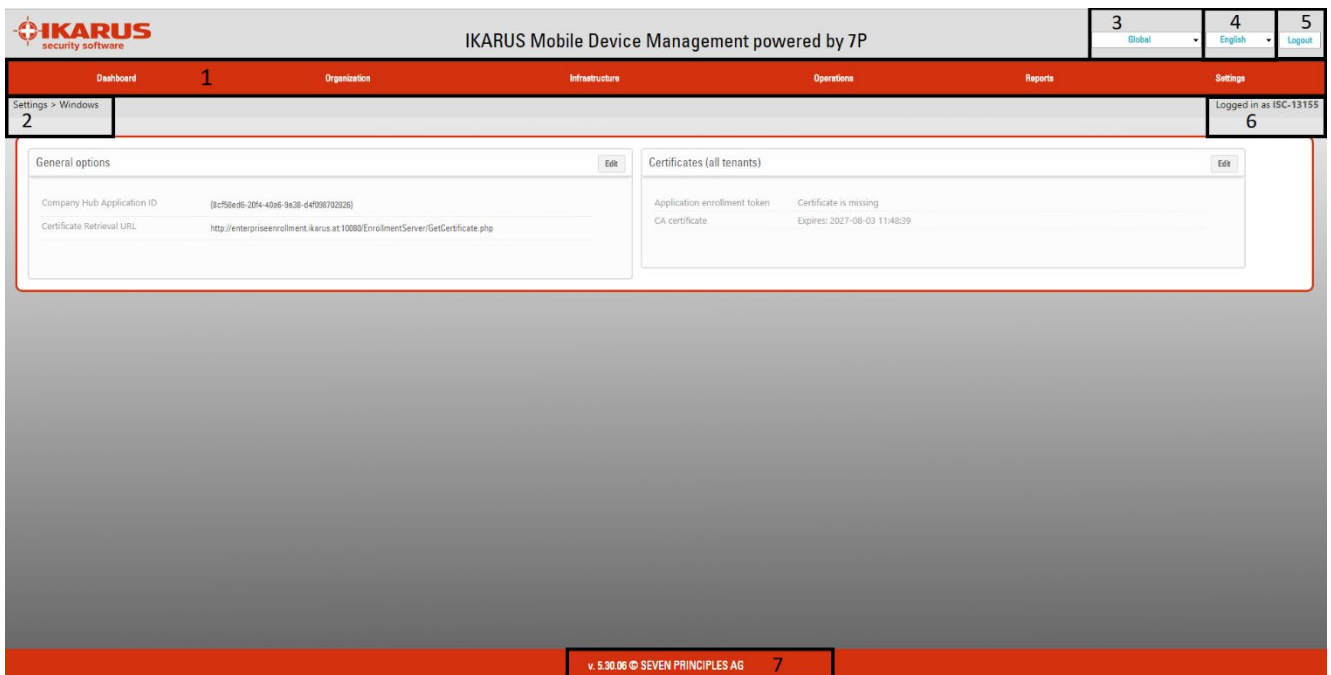


The initial tenant administrator password is configured by your IKARUS mobile.management service provider. If you have difficulty logging in to your account, please contact your provider who will guide you through the process.

Once logged in, the task for the tenant administrator is to create additional administrator accounts, define a group hierarchy that is convenient for their organisation and add users.

3.1.1 Initial login

After initial login – Navigate to **Settings > Base**



The screenshot displays the IKARUS Mobile Device Management interface. At the top, the header includes the IKARUS logo, the text 'IKARUS Mobile Device Management powered by 7P', and navigation options for 'Global', 'English', and 'Logout'. Below the header is a main navigation bar with tabs for 'Dashboard', 'Organization', 'Infrastructure', 'Operations', 'Reports', and 'Settings'. The 'Settings' tab is active, and a breadcrumb trail shows 'Settings > Windows'. The main content area is divided into two panels: 'General options' and 'Certificates (all tenants)'. The 'General options' panel shows fields for 'Company Hub Application ID' and 'Certificate Retrieval URL'. The 'Certificates (all tenants)' panel shows 'Application enrollment token' and 'CA certificate' details. A footer bar at the bottom indicates the version 'v. 5.30.06 © SEVEN PRINCIPLES AG'.

The IKARUS mobile.management UI consists of the following key elements:

1. Main menu navigation bar (click each header to display drop down sub menu options)
2. Breadcrumb – where you currently are
3. The name of the tenancy
4. UI display language selection
5. Logout button
6. User account detail
7. Version on IKARUS mobile.management server

3.1.2 Create additional administrator accounts

In this example we will use a tenancy called EMM01

Navigate to **Settings > Base > Admins**

- Select **Add new** from the Admins configuration (The Add new Admin configuration template will be shown)
- **Insert** the Username, password and Repeat new password in the fields provided.
- From the “Role” drop-down list, select either the preconfigured Administrator, Help desk administrator, or Read only administrator.
- Select the tenancy (EMM01) in the Tenants scrollable list.
- Ensure that a corporate email address is inserted in the Email field (used for password recovery)
- Finally select Two-factor authentication – **Off**.
- Select **OK**.

The new Admin account with the defined Admin roles will be created.

Logout of the IKARUS mobile.management server. Login with the newly created Admin account.

Login to the IKARUS mobile.management server using the newly created administrator username and password. You will be logged into the EMM01 tenancy.

3.2 Creating Hierarchies and Groups

Hierarchies and groups allow the IKARUS mobile.management system administrator to define an organisation structure using logical levels to either reflect their own organisational structure or to create a new organisational structure to assist with their mobile device management.

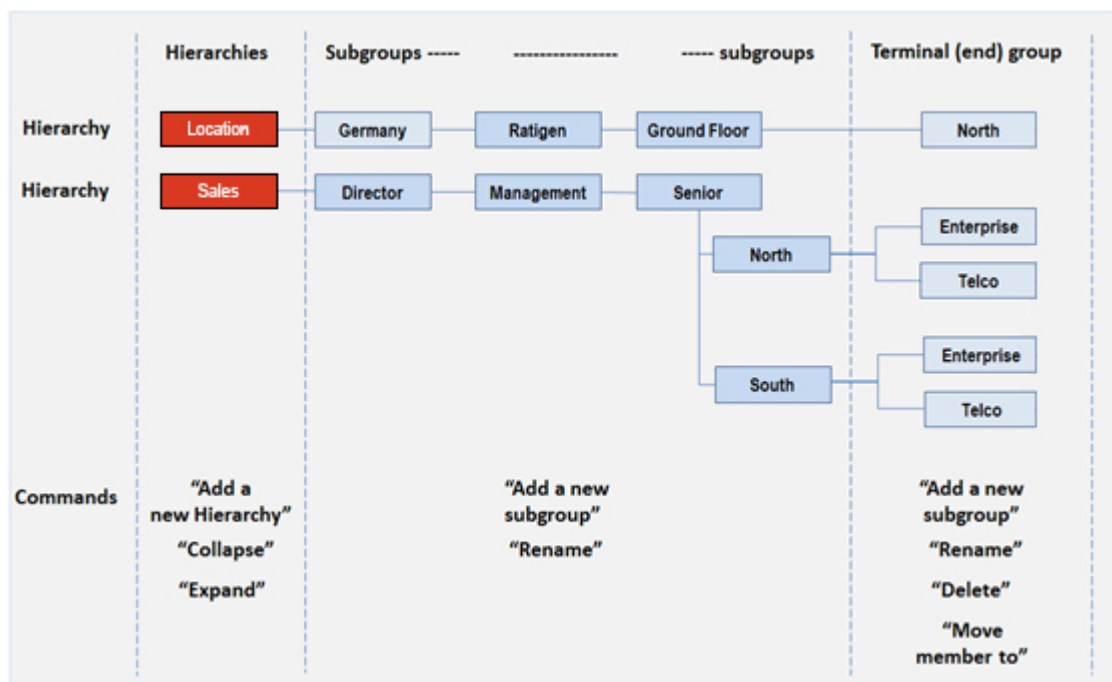


Figure 4 Hierarchy & Groups command summary

3.2.1 Creating a simple group hierarchy

Navigate to **Organization > Hierarchy & Groups**

Select **“Add new hierarchy”** - Insert **“Sales”** in the pop-up provided. **“Sales”** will appear on the hierarchy.

Select **“Add a new subgroup”** – Insert **“North”** in the pop-up provided. **“North”** will appear in the Sales hierarchy.



Selecting **“Sales”** again, then selecting **“Add a new subgroup”** – Insert **“South”** in the pop-up provided. **“South”** will appear in the **“Sales”** hierarchy

3.3 Adding a new user

Navigate to **Organization > Users and devices > Add user**

First name, last name and either email address **OR** UserID are **mandatory** fields that are required when adding a new user.

User information fields

Detail	Description
First name*	The first name of the new user
Last name*	The surname of the new user
Email address*	An email address of the new user (Either Email is mandatory OR UserID)
UserID*	A unique numeric code of the manually assigned to the user (Either Email is mandatory OR UserID)
WINDOWS username	If a WINDOWS user, then a WINDOWS username is required
Password	If a WINDOWS user, then a password is required
Assigned mobile number	The MSISDN number of the SIM card given to the user by the administrator (Multiuser must be enabled)
Group allocation	The groups that the new user will be a member of
Custom Parameters	User assigned custom parameters, the user's device(s) inherit these values

Table 1 User details

On completion of the edit, the administrator must select **“Save,”** to update the user details to the IKARUS mobile.management server.

3.3.1 Deleting a user

Navigate to **Organization > Users and devices > Username**
Select **Delete** from the user detail window



All associated details, including devices, applications, configurations installed, and history will be deleted from the IKARUS mobile.management server.

3.4 Adding multiple users via CSV file import

The CSV import utility will allow the administrator to import from a single user to many thousands of users by presenting a well-formed CSV file to the IKARUS mobile.management server "CSV import" facility.

The following is a basic example CSV file, which has been exported "saved as CSV" from Microsoft Excel, selecting the "comma" as the CSV delimiter value. The column headers are case sensitive.

msisdn	lastName	firstName	email	enrollEmail
442091233322	Lastname2	Firstname2	f2.v2@l.com	f2.v2@enroll.com
442091234433	Lastname3	Firstname3	f3.v3@l.com	f3.v3@enroll.com
442091235544	Lastname4	Firstname4	f4.v4@l.com	f4.v4@enroll.com

Navigate to **Organization > Users and devices**, then select the "**CSV import**" button. The CSV import window will be presented.

The "**Choose File**" button will allow the administrator to explore their file system for the prepared CSV file. Once selected, the name of the CSV file will be displayed adjacent to the "**Choose File**" button.

Selecting the "Import" button on the CSV pane will commence the CSV import feature.



The time to import user information from a prepared CSV file will depend upon the number of records within the CSV file. Once the CSV import has completed, the users will be available to add devices.



If User ID is used as the preferred (mandatory) identification method (See **Settings > Base > Common options (all tenants) > User identification**) then replace the CSV header "email" with userID.

4 Adding a basic Android device

The IKARUS mobile.management server requires the installation and authentication of the Android IKARUS mobile.management client application onto the physical device before device management can commence. This process is termed enrollment. The enrollment process slightly differs for Android Enterprise, Samsung KNOX, Samsung KME, and basic Android devices.

A basic (Generic) Android device usually utilises the Google Android API feature set.

- With Mobile phones, enrollment begins when the user opens a SMS text message sent to the device by the IKARUS mobile.management server administrator.
- With Wi-Fi devices, enrollment begins when the user opens an email message sent to the user by the IKARUS mobile.management server administrator.

4.1.1 Basic Android SIM device SMS enrollment

Navigate to **Organization > Users and devices > Designated_User > Add device**

The New device data configuration window will be displayed from which the user must select the **Android** tab. (More Android configuration details will be displayed once selected.).

Insert a friendly name in the device name field, and enter a valid mobile phone number (using International format e.g. +370)

Once the mobile phone number has been inserted, the Enroll via SMS button, at the bottom of the New device data configuration window will become active.

Select the “**Enroll via SMS**”

A SMS text message will be sent to the phone number provided. The SMS message contains the download hyperlink for the IKARUS mobile.management Client application that must be installed on the user's device. Embedded in the SMS text message is an encrypted activation code, used by the IKARUS mobile.management client application to authenticate and communicate with the IKARUS mobile.management server.

The user on receipt of the text message,:

- Must open the text message and tap/select the hyperlink URL. Once the hyperlink is selected, the IKARUS mobile.management client will be automatically downloaded to the device.
- May receive a warning that their device will not install applications from unknown sources, and present an internal link to the application manager.
- Must allow installations of applications from unknown sources.



During the installation process the user may be requested by the application to accept default permissions, Terms and Conditions and licensing requests. The user must accept all requests as part of the installation process.

Once the IKARUS mobile.management client application has installed onto the device it will automatically authenticate with the IKARUS mobile.management server. The IKARUS mobile.management client will display that it is **Activated**, once authentication with the IKARUS mobile.management server has completed.

The IKARUS mobile.management administrator may now view the (returned) device details which have been communicated to the IKARUS mobile.management server by the IKARUS mobile.management client.

Navigate to **Organization > Users and devices > Designated_User > Newly_added_device**

Inspect the Inventory, Details, Actions, History, Installations and SIM card windows.

4.1.2 Basic Android Wi-Fi device email enrollment

Email enrollment has been designed for Wi-Fi devices. The enrolling device must be capable of scanning a QR code presented in the enrolling email. It is advisable for the recipient to open the enrollment email on their laptop or workstation, whilst having the enrolling Wi-Fi device with them.

Navigate to **Organization > Users and devices > Designated_User > Add device**

The New device data configuration window will be displayed from which the user must select the **Android** tab. (More Android configuration details will be displayed once selected.).

Insert a friendly name in the device name field. No other information is necessary. The email will be sent to the registered users corporate email address as defined in **Organization > Users and devices > Designated_User > Email**

At the bottom of the New device data configuration window select the “**Enroll via email**” An email, containing the download hyperlink for the IKARUS mobile.management Client application and a QR code, will be received by the designated user.

The user on receipt of the email message:

- Must open the email on their device and tap/select the hyperlink URL. Once the hyperlink is selected, the IKARUS mobile.management client will be automatically downloaded to the device.
- Must also open the email on another device – laptop, workstation or even another mobile device so that the QR code embedded in the enrollment email can be displayed.
- May receive a warning that their device will not install applications from unknown sources, and present an internal link to the application manager.
- Must allow installations of applications from unknown sources.

The IKARUS mobile.management client will install.

During installation, the activation screen will become available. The user must select “Activate with QR code” and scan the QR code received in the enrollment email, by the IKARUS mobile.management client application.

The user will then be asked to supply a security code – which is typically 1234.



During the installation process the user may be requested by the application to accept default permissions, Terms and Conditions and licensing requests. The user must accept all requests as part of the installation process.

Once the IKARUS mobile.management client application has installed onto the device it will automatically authenticate with the IKARUS mobile.management server. The IKARUS mobile.management client will display that it is **Activated**, once authentication with the IKARUS mobile.management server has completed.

The IKARUS mobile.management administrator may now view the (returned) device details which have been communicated to the IKARUS mobile.management server by the IKARUS mobile.management client.

Navigate to **Organization > Users and devices > Designated_User > Newly_added_device**

Inspect the Inventory, Details, Actions, History, Installations and SIM card windows.

5 Adding an iOS device

When a system administrator adds an iOS device to the IKARUS mobile.management server, an email (or SMS text message if SIM enabled device) is generated containing a hyperlink URL which when opened on the user's iOS device, will instruct the iOS device in the installation of the Apple IKARUS mobile.management profile. Once the Apple IKARUS mobile.management profile is installed, the IKARUS mobile.management client may be added to the device.

5.1.1 Adding an iOS SIM device

Navigate to **Organization > Users and devices > Designated_User > Add device**

The New device data configuration window will be displayed from which the user must select the **iOS** tab.

Insert a friendly name in the device name field, and enter a valid mobile phone number (using International format e.g. +370)

Once the mobile phone number has been inserted, the **Enroll via SMS button**, at the bottom of the New device data configuration window will become active.

Select the **“Enroll via SMS”**

A SMS text message containing the iOS profile hyperlink will be sent to the device. The user then selects the hyperlink within the SMS text message.

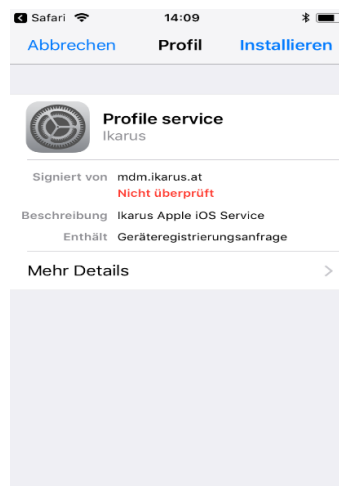


Figure 5 URL link opened to the profile process.

A new web page will open on the user's device. The user may either Install the IKARUS mobile.management profile, or cancel the operation. The user will be challenged for the devices passcode. When the passcode is entered correctly, the IKARUS mobile.management profile will be installed.

The IKARUS mobile.management administrator may now view the (returned) device details which have been communicated to the IKARUS mobile.management server the IKARUS mobile.management profile.

Navigate to **Organization > Users and devices > Designated_User > Newly_added_device**
Inspect the Inventory, Details, Actions, History, Installations and SIM card windows.

6 Adding Android Enterprise functionality

Introduction Android for Enterprise is a free feature of Google, which can be used in many mobile devices with the mobile operating system Android. This feature allows you to activate a so-called work profile, which provides a way to clearly separate private and corporate data. An overview of currently supported devices can be found at the end of this document.

6.1 Requirements

A Gmail account is required in to enroll your IKARUS mobile.management server instance (whether global or tenant instance) into Android for Enterprise. If you do not have one, create a generic account (based on your business) that your company's authorized IT administrators have access to. For example, you could use your company name (s) with an AfE (for "Android for Enterprise") suffix. Private (personal) accounts should not be used.

6.2 Preparation

Before you can start Android for Enterprise on your mobile devices, consider whether your IKARUS mobile.management installation will use Android for Enterprise globally, allowing all tenants to use one Android for Enterprise account, or through multiple individual tenants, each tenant having registered their own Android for Enterprise account.

6.2.1 Global tenant check

- 1) Log into the IKARUS mobile.management server.
- 2) Ensure the "Global" tenancy is currently displayed.
- 3) Navigate to **Settings > Android > Android Enterprise** and make sure the Enterprise enrollment service authentication token is present and visible (allows communication between the IKARUS mobile.management server and Googles enterprise) file is present.

Please contact IKARUS if no enrollment service authentication token is displayed.

6.2.2 Tenant check

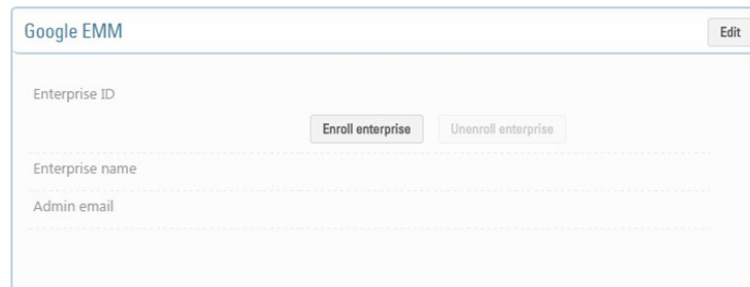
- 1) Log into the IKARUS mobile.management server.
- 2) Ensure the correct tenancy is currently displayed.
- 3) Navigate to **Settings > Android > Android Enterprise** and make sure the Enterprise ID field is displaying a completion token.

Please contact IKARUS if no completion token is displayed.

6.3 Enroll enterprise

The enrollment process for both a Global tenant and customer tenant is the same:

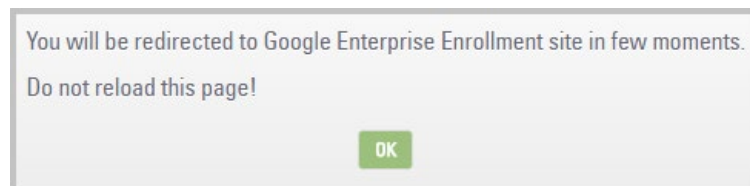
- 1) Navigate to **Settings > Android > Android Enterprise** and select the **Enroll enterprise** button



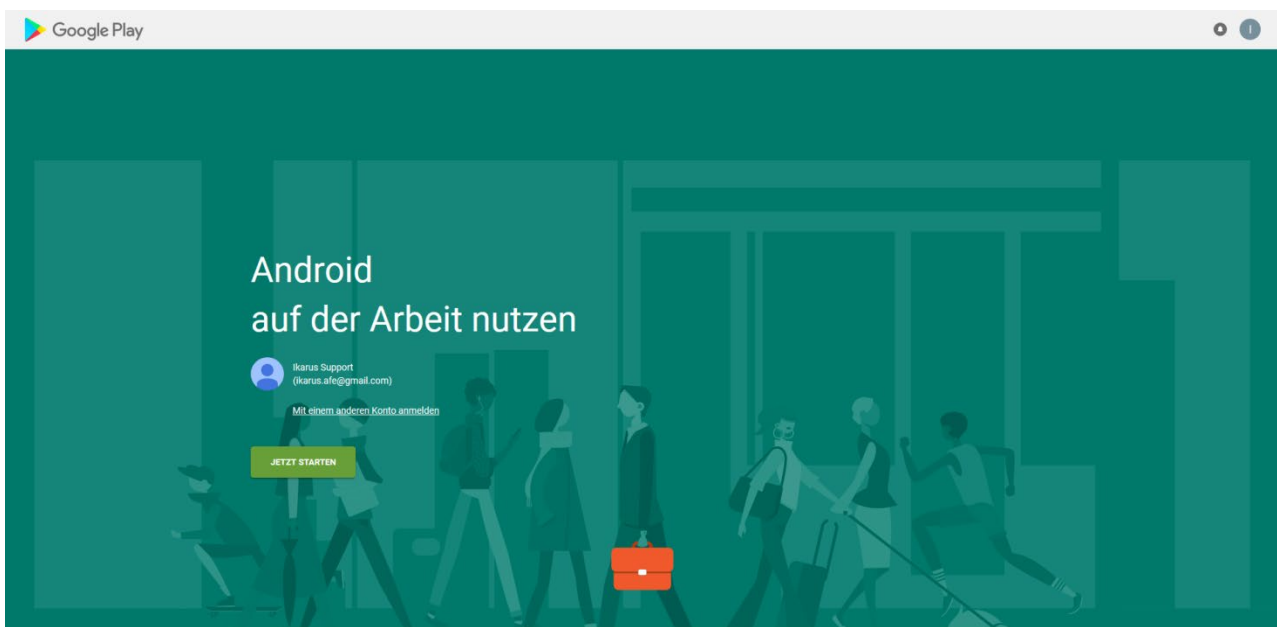
The screenshot shows a form titled "Google EMM" with an "Edit" button in the top right corner. The form contains the following fields and buttons:

- Enterprise ID: A text input field with a button labeled "Enroll enterprise" to its right and a button labeled "Unenroll enterprise" to its right.
- Enterprise name: A text input field.
- Admin email: A text input field.

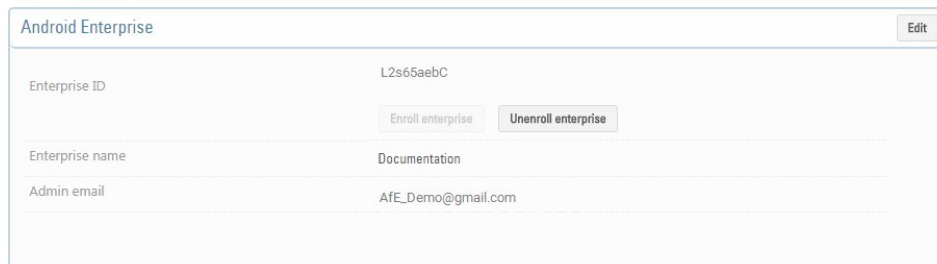
- (2) The following window will be briefly displayed and you will be redirected to Google – press OK



On selection the following Google interface will be seen. Ensure that the correct Google account is being used prior to "Getting started".



If an alternate account has been allocated, then select “Sign in with a different account” – insert the username and password.
 After a few seconds you will automatically be redirected to the IKARUS mobile.management system and more information will be displayed in the Android Enterprise window.



Android Enterprise		Edit
Enterprise ID	L2s65aebC	
	<input type="button" value="Enroll enterprise"/> <input type="button" value="Unenroll enterprise"/>	
Enterprise name	Documentation	
Admin email	AfE_Demo@gmail.com	

The IKARUS mobile.management Google EMM registration screen displays the following:

- Enterprise ID** – returned from Google’s infrastructure
- Enterprise name** – the friendly name used to enroll the enterprise
- Admin email** – the email address of the enrolling account



Selecting the “Unenroll enterprise” will disassociate all account details, purchases and deployments from the IKARUS mobile.management server. This account details and any outstanding balances will still be paid for by the account used to enroll the enterprise.

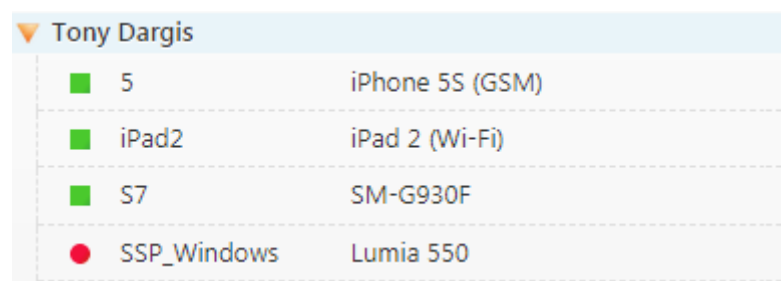
This completes all preparations and allows you to start the device rollout.

6.4 Device rollout

This section assumes that the IKARUS mobile.management client 5.27.02 or above is installed into a *work profile* capable device, is online to the IKARUS mobile.management server, activated and has a valid data connection.

To enable the Android Enterprise Profile (work profile) on Android devices, please do the following:

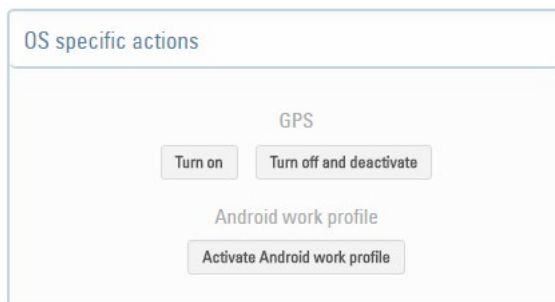
- 1) Enroll the device as usual by installing and activating the IKARUS mobile.management Client on the device.



▼ Tony Dargis	
■ 5	iPhone 5S (GSM)
■ iPad2	iPad 2 (Wi-Fi)
■ S7	SM-G930F
● SSP_Windows	Lumia 550

On successful completion of device enrollment do the following:

- 2) Navigate to **Organization > Users and devices > User > Device > Actions > OS specific actions**
- 3) Select the "Activate Android Work Profile" button.

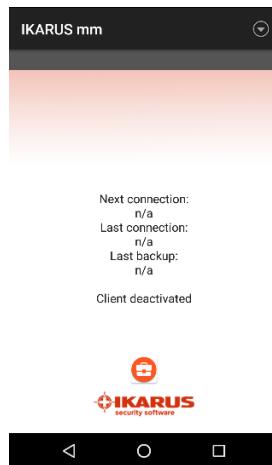


- 4) An additional device (work profile) entry in the list is automatically created for the selected device.

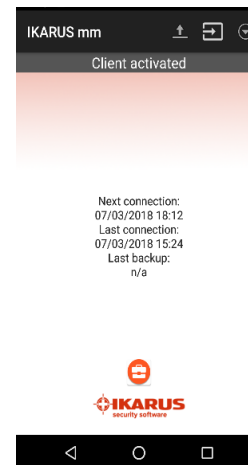
Tony Dargis	
5	iPhone 5S (GSM)
iPad2	iPad 2 (Wi-Fi)
S7	SM-G930F
S7 (work profile)	SM-G930F
SSP_Windows	Lumia 550

The Android Work profile icon (briefcase) will appear on the devices notification bar, which when pulled down will reveal the IKARUS mobile.management server notification message.

- 5) At the next device connection the activation of the device (work profile) commences.
 - a. Accept the terms and conditions
 - b. Confirm the setup of the work profile
 - c. Newer devices are already encrypted by default. Older devices that support the device (work profile) will be encrypted as part of the device (work profile) initialisation. Without device encryption, the work profile cannot be activated.
 - d. After successful encryption (if required), the device restarts and activation of the work profile will continue. If this process does not start automatically, please also check any notifications in the notification bar (at the top of the device).
 - e. The work profile will now be set up and a dedicated IKARUS mobile.management client for this profile will be activated.



Work profile IKARUS mobile.management client begins activation



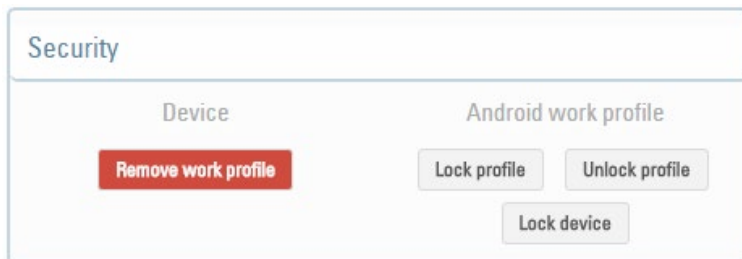
Work profile IKARUS mobile.management client activated

- f. After successful activation of the work profile client activation a brief case symbol will be displayed on the IKARUS mobile.management client. All applications within the device (work profile) will also display the brief case symbol on their application icon.
- g. In the IKARUS mobile.management user interface, you also see that the IKARUS mobile.management client is enabled for the work profile.

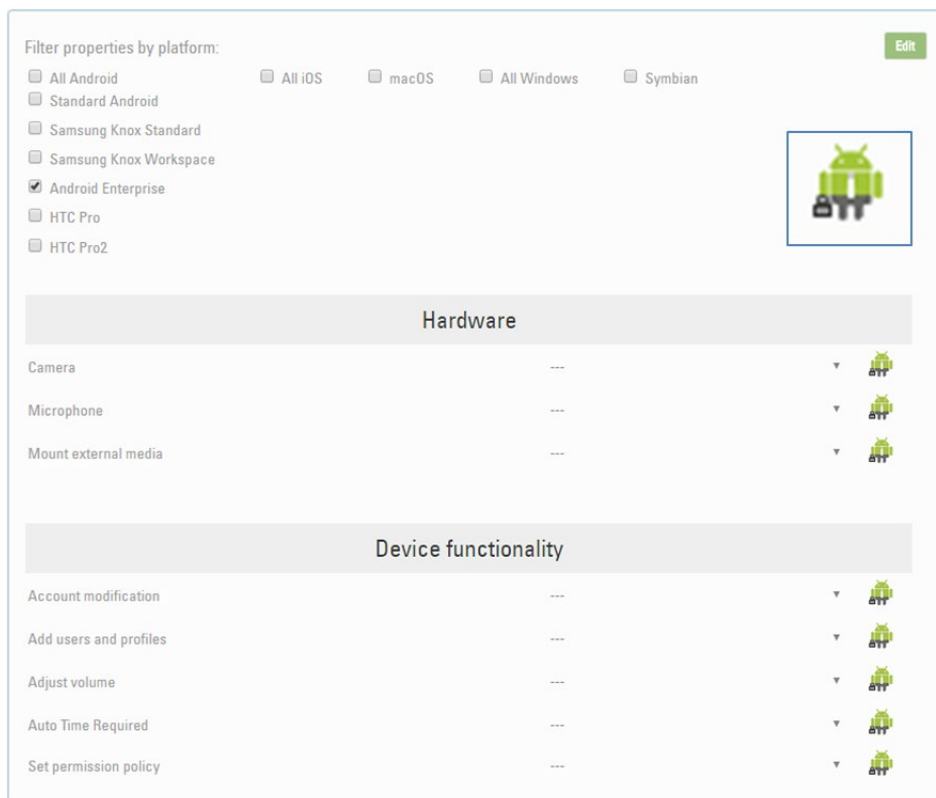
Tony Dargis	
5	iPhone 5S (GSM)
iPad2	iPad 2 (Wi-Fi)
S7	SM-G930F
s7 (work profile)	SM-G930F
SSP_Windows	Lumia 550

This entry is considered as an independent (virtual) device and can be managed independently from the actual physical device. For this reason, it is provided with its own inventory and administration area.

Navigate to **Organization > Users and devices > User > Device (work profile)> Actions > Security**



Configuration parameters supported for the Android for Enterprise work profile are marked with this icon. You can therefore create custom configuration templates for your Android for Enterprise work profiles.



You can therefore create custom configuration templates for your Android for Enterprise work profiles.

6.5 Official Device List

For an up to date version of Android for Enterprise compatible devices visit <https://www.android.com/enterprise/devices/>

7 Managed Google Play (custom) store layout editor

The Play Store (work profile) contains two discrete application locations. Store home which is

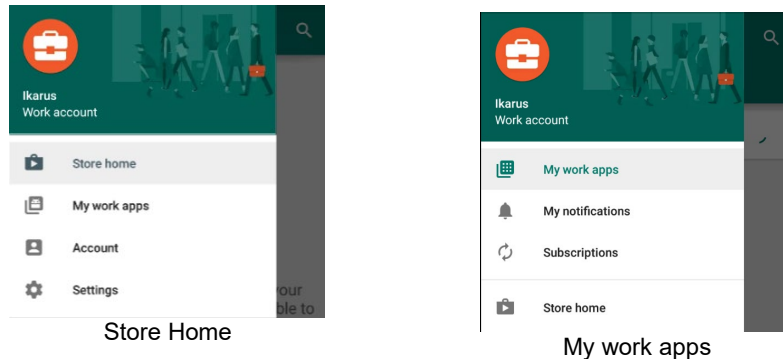


Figure 6 Device Play Store (work profile) Works account view

The IKARUS mobile.management server Managed Google Play store (custom) layout editor - allows the administrator to present, on the users device, the available approved Work profile applications in an organised and preferred manner.

The initial managed Google Play store layout editor has one default page, Page 1, with no applications listed.

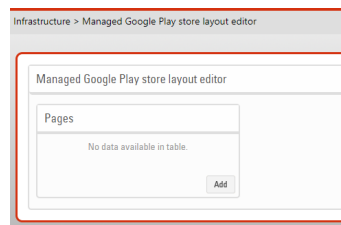


Figure 7 Default (as shipped)

The managed Google Play store editor is an optional component to the IKARUS mobile.management server that requires either the Global scope of the IKARUS mobile.management server or the current tenant scope (the administrator's tenancy) of the IKARUS mobile.management server to have an enrolled Google EMM enterprise before the Managed Google Play Store editor becomes available.

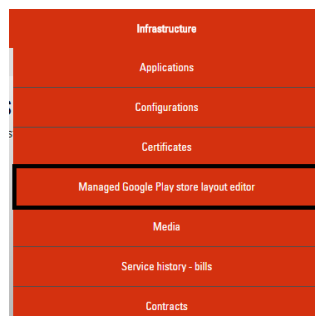


Figure 8 Google Play Store (custom) layout editor tab

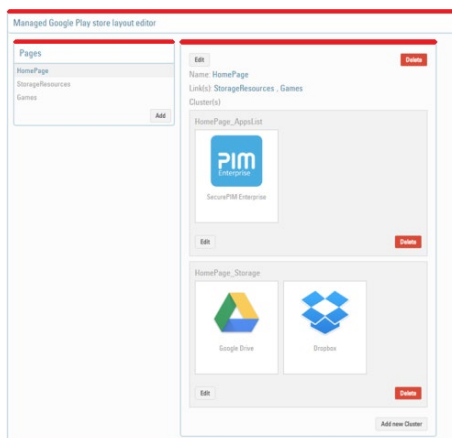


A Global scope or Tenancy Google EMM enterprise account must be present before the Managed Google Play store layout editor can retrieve and display information from the managed Google Play store.

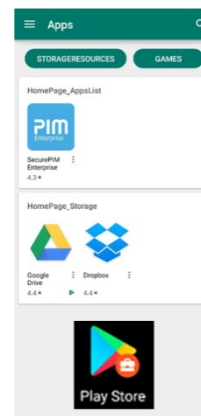
7.1 Using the managed Google Play store (custom) layout editor

The default Managed Play Store layout editor displays 1 page, named “Page 1” **which cannot be deleted**. The page name, however, may be edited. The layout editor consists of:

- Pages – To assist in logical organisation of applications
 - Add pages - These pages may be renamed at any time.
 - Delete pages – Delete any page (except the default Page 1) – All cluster and application link information will be deleted. The applications will not.
 - Rename page titles – The edited page names remain within the Only pages can contain links to other pages
- Links (to other pages)
 - Add Links to created pages (except to its own page)
 - Delete links to other created pages.
- Clusters (Logical groupings of applications)
 - Pages may contain one or more clusters
 - Each cluster may contain one or more applications
 - Each cluster may be deleted. The link to any applications will also be deleted. The applications will not.
- Applications (Approved Applications resident on Google Play Store)
 - Applications made available through the IKARUS mobile.management server Applications
 - Applications made available through the IKARUS mobile.management server Application Configuration



IKARUS mobile.management – Play Store layout top view



Device - Play Store(work profile)

Figure 9 IKARUS mobile.management Server and Device appearance

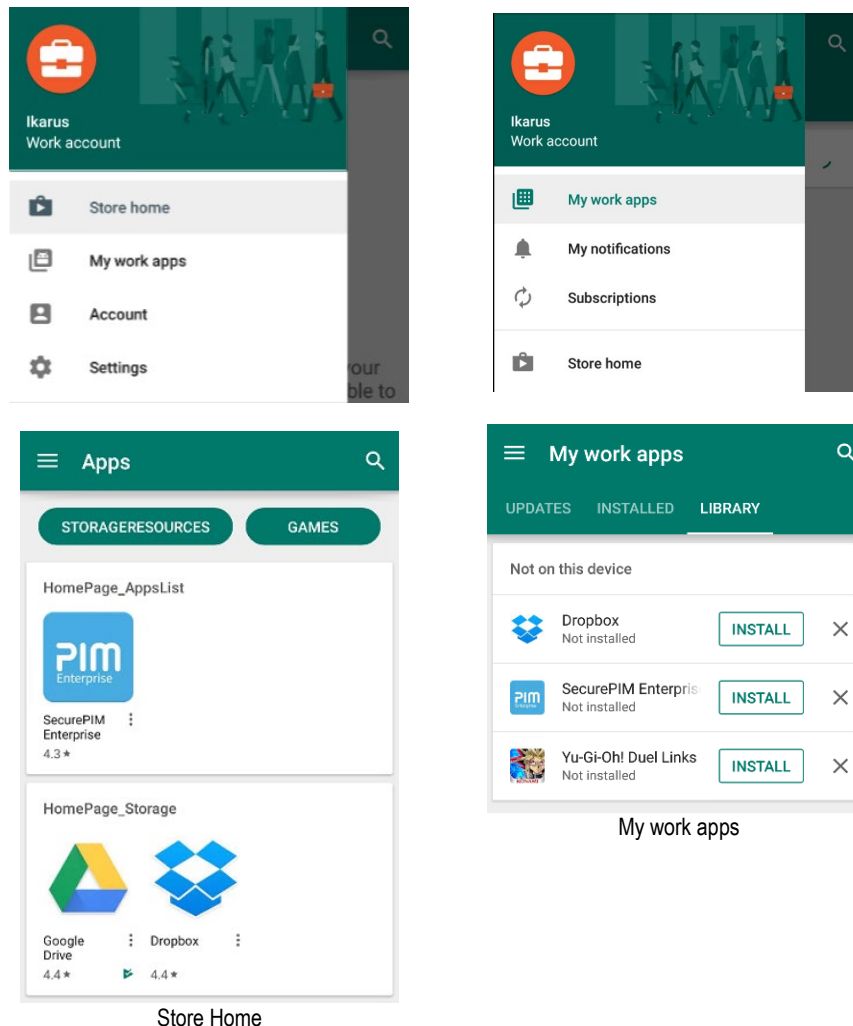


The user may, at any time, navigate to their Play Store (work profile) and access their “My work apps” which will display all the apps that have been added to the Play Store account by the Google Play Store administrator. The user may select any of the approved apps and install them directly onto their device.

7.2 Work profile – Device view

Once the Work profile has been installed, and the managed Google Play account has been activated, then the user has the opportunity to navigate to the managed Play Store by selecting - Store Home or the managed Play Store by selecting – My work apps

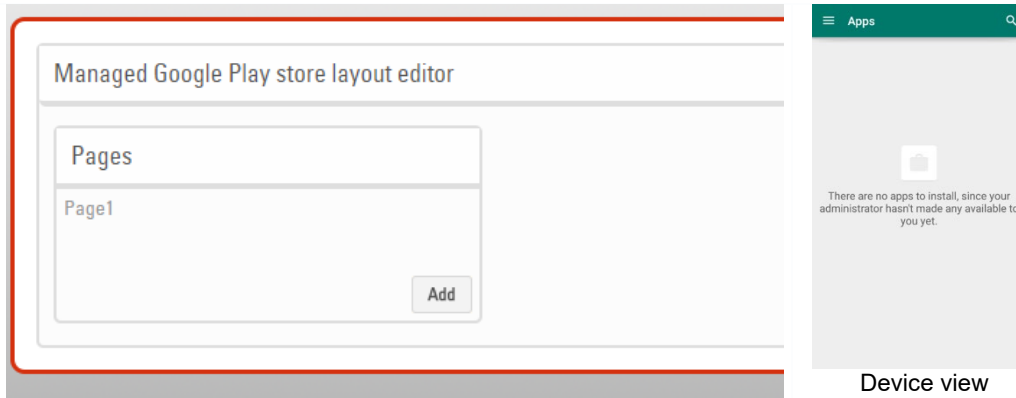
On the user’s device - navigate and open the Play Store (work profile)



The IKARUS mobile.management server Managed Google Play store layout editor allows the administrator to present, on the user’s device, the available Work profile applications in an organised and preferred manner, and can only influence the appearance of the “Store home” on-device display.

7.2.1 Google Store (custom) layout editor - walkthrough

Pages may be added to the managed Google Play Store layout at any time. Pages, along with their contents (links to Google Play Store apps) may also be removed at any time.



Layout editor view

7.2.2 Rename Page 1 (default) to Homepage

Navigate to **Managed Google Work Store layout editor > Pages > Page 1 > Edit**

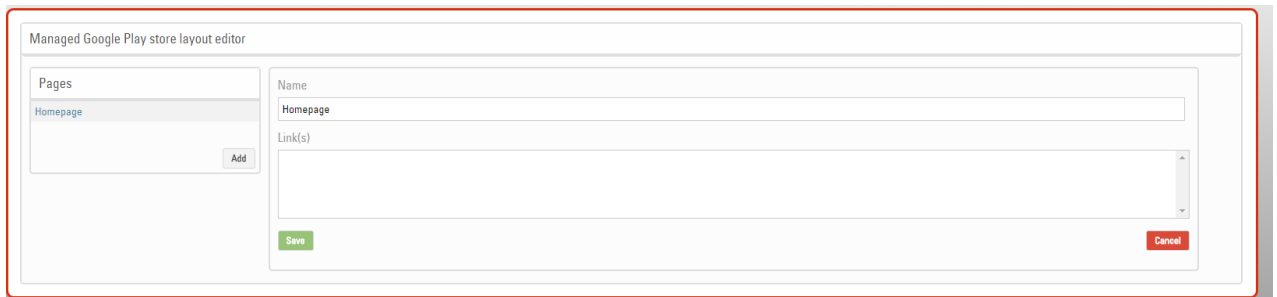


Figure 10 Managed Google Work Store layout editor - Page 1 edit

Insert a friendly name – Homepage is used in this example, but the name of your organisation can equally be used. Then select Save.

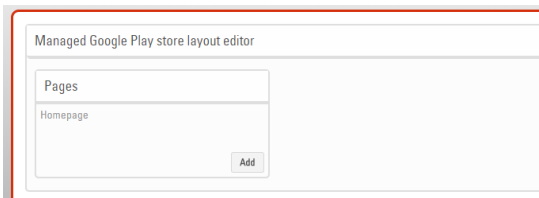


Figure 11 Managed Google Work Store layout editor - Page 1 renamed

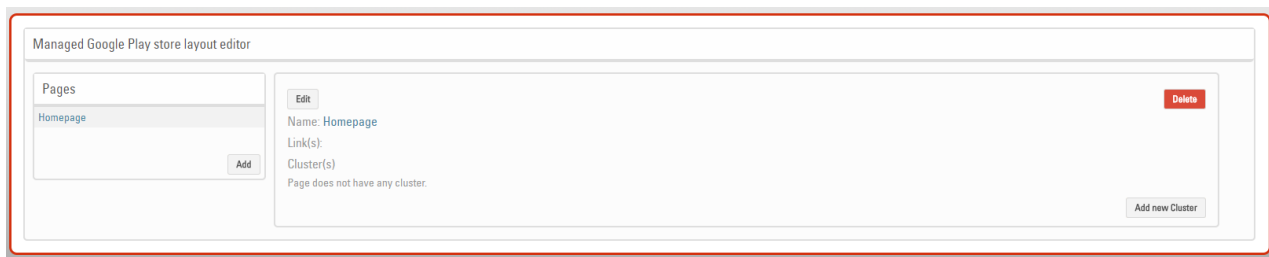
The default page has been successfully changed to “Homepage”

7.2.3 Example 1

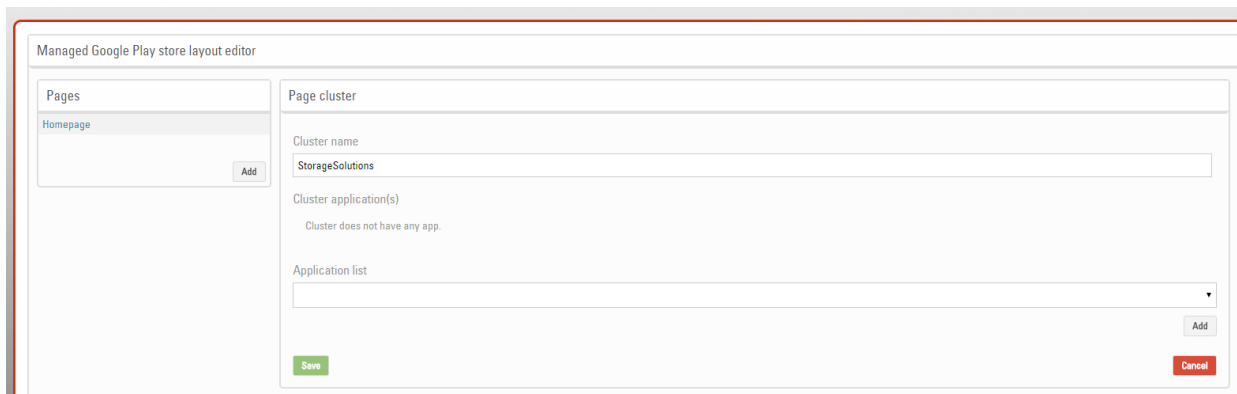
In this example we will describe how to:

- Change the name of the default page “Page 1” to “Homepage”
- Add a named cluster to the page – „Homepage“
- Then Add an application to the page - “Homepage“

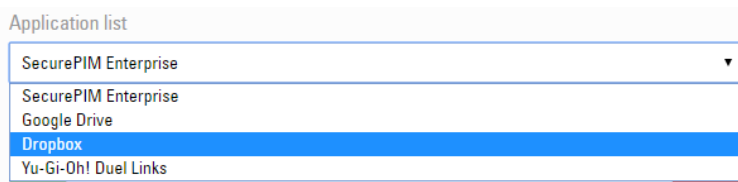
Navigate to **Managed Google Work Store layout editor > Pages > Page 1 > Edit > Add new cluster**



Insert a friendly name into the Cluster name field – in this example StorageSolutions



Then select the Application list drop down.



A list of applications that have been approved on the Google Play Store and any Android application that has been loaded into the IKARUS mobile.management server from the Play Store (and approved) will appear.

Select an application, in this case Dropbox, and Select Add

The application icon will be displayed in the Cluster application(s) field – Then press Save, to save the application link to the StorageSolutions cluster.

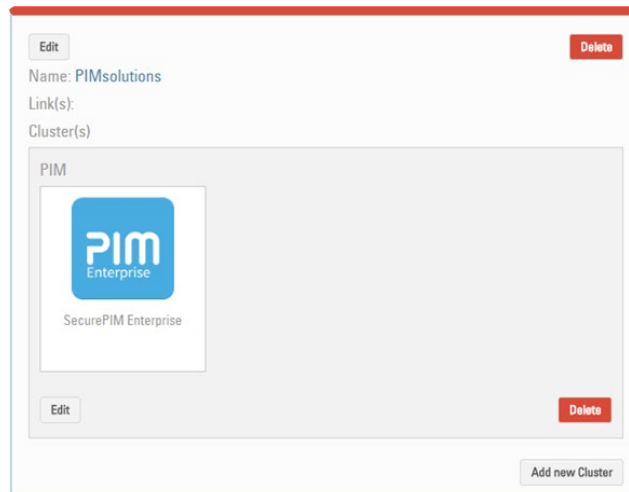
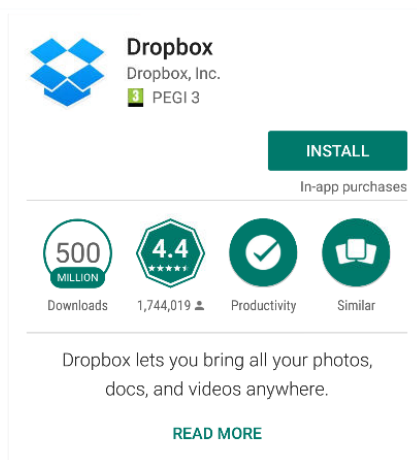
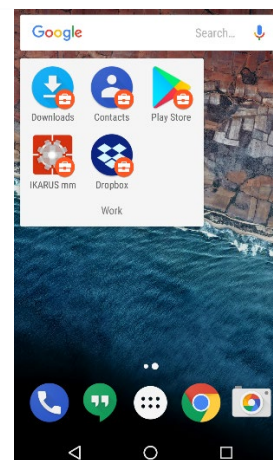


Figure 12 Managed Google Work Store layout editor - Add app

If the customer selects the Dropbox icon, then they will be invited to install the application onto their device.



Device view – install?



Device view - installed

The application has been installed into the work profile of the device, and will be removed if the work profile is deleted manually by the user (Accounts – delete Work) or a Device Wipe has been issued by the IKARUS mobile.management administrator on the device (work profile).

All apps installed via Google Play for Work are installed without use of any local or user Google account as well as user also not prompted for app permissions since this was pre-accepted by the admin when approving the app.

7.3 Example 2

In this example we will be – Adding a page, link and application
For Example 2 – duplicate the following (using your own approved applications when possible)

Navigate to **Managed Google Work Store layout editor > Pages > Add**

1. Add – Name – PIMsolutions, Link Homepage then Save
2. Select Homepage > Edit – Highlight Link(s) and select PIM solutions – then Save
3. Pages > Select PIMsolutions – Add new cluster
4. Insert friendly cluster name PIM
5. From the application drop down list – select Secure PIM Enterprise – Add

The users work profile Google Play Store UI is typically updated when the IKARUS mobile.management client connects to the IKARUS mobile.management server.

Please note that an administrator may use the Managed Google Play Store layout editor:

Pages

- Add pages - These pages may be renamed at any time.
- Delete pages – Delete any page (except the default Page 1) – All cluster and application link information will be deleted. The applications will not.
- Rename page titles – The edited page names remain within the Only pages can contain links to other pages

Clusters

- Pages may contain one or more clusters
- Each cluster may contain one or more applications
- Each cluster may be deleted. The link to any applications will also be deleted. The applications will not.

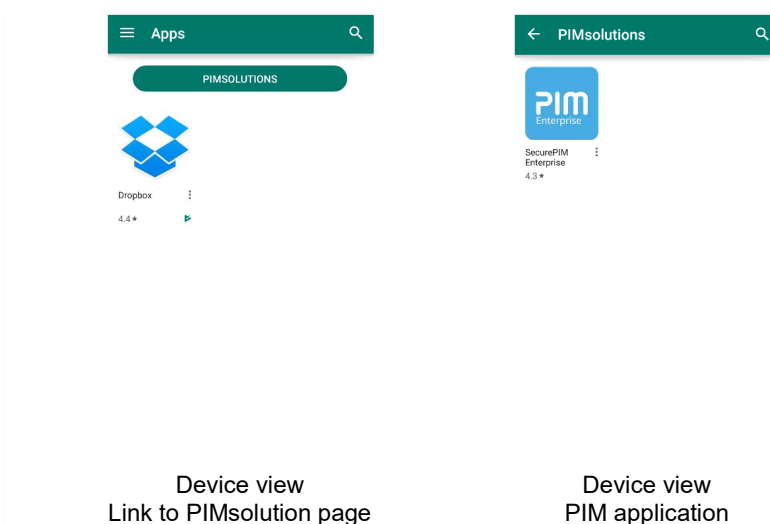
Links (to other pages)

- Add Links to created pages (except to its own page)
- Delete links to other created pages.

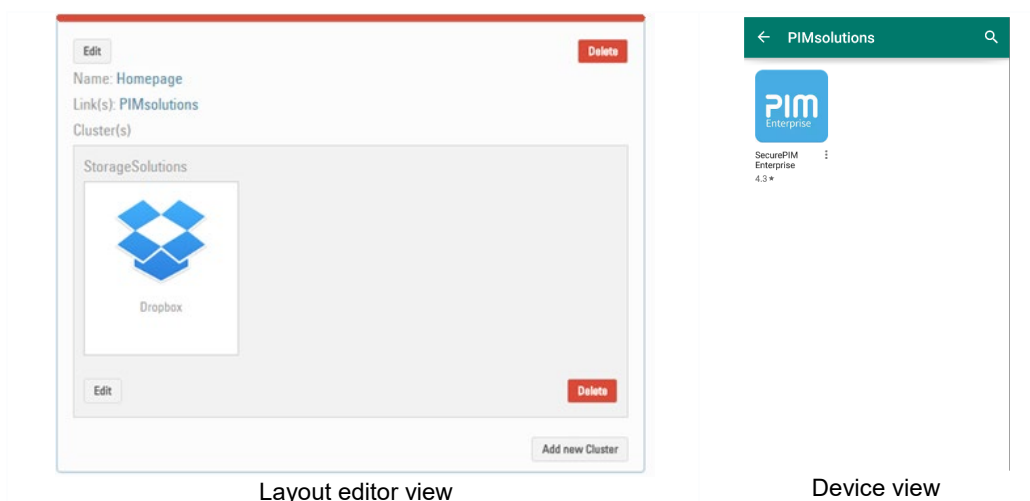


There is no (known) restriction to the number of Pages, Clusters and Links that may be created with the managed Google Play Store layout editor. This facility has been integrated into the IKARUS mobile.management server so that users can readily find (and install) company approved applications with ease. It is suggested, therefore, that a logical approach to the design of the company approved application layout is desirable:

Example 2 results as viewed by the users device.



Example 2 – Result of Adding link, Cluster name and application



The application is now available for the user to install onto their device.

Tab	Description
Add	Adds a new page
Delete	Deletes the page (excluding Page 1 – Home page)
Name	Select the page name – the to rename the page name – to add or remove Links (to other pages)
Add new cluster	Adds an additional cluster, which can be named, and application links added

Retrieves all application information from Google

List of changes

Version	Date	Changes	Reason	Author
1.0	2017-11-26	Version release	5.30	Tony Dargis