IKARUS

mobile.management

Quick Start Guide

1. Inhalt

^Home

2. Abbildungsverzeichnis

^Home

3. Allgemeines

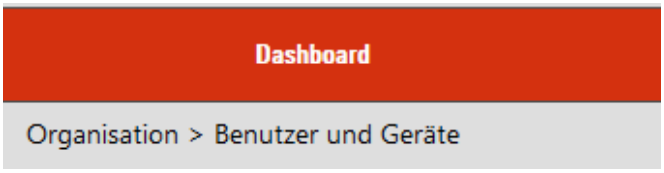
3.1. Umfang

Bei diesem Quick Start Guide handelt es sich um eine Zusammenstellung aller Schnellstartsegmente in einem Dokument, mit dem Sie als Benutzer unkompliziert auf alle Informationen zugreifen können, die Ihnen schnellstmöglich zum produktiven Einsatz des IKARUS mobile.management-Servers verhelfen.

4. Navigation

4.1. Breadcrumb

In der linken oberen Ecke des User Interface zeigt ein Breadcrumb den aktuellen Standort innerhalb des IKARUS-mobile.management-Systems an.



Der Breadcrumb hat nur Hinweischarakter und ist kein aktiver Link.

4.2. Layout der Benutzeroberfläche

Die Navigation auf dem IKARUS mobile.management-Server erfolgt durch Auswahl eines Menütitels (Dashboard, Organisation, Infrastruktur, Abläufe, Berichte und (System-)Einstellungen) auf der horizontalen Hauptmenü-Navigationsleiste der Benutzeroberfläche des IKARUS mobile.management-Servers. Nach Auswahl eines Titels erscheinen die verknüpften Menüpunkte in vertikalen Dropdown-Untermenüs.

^Home

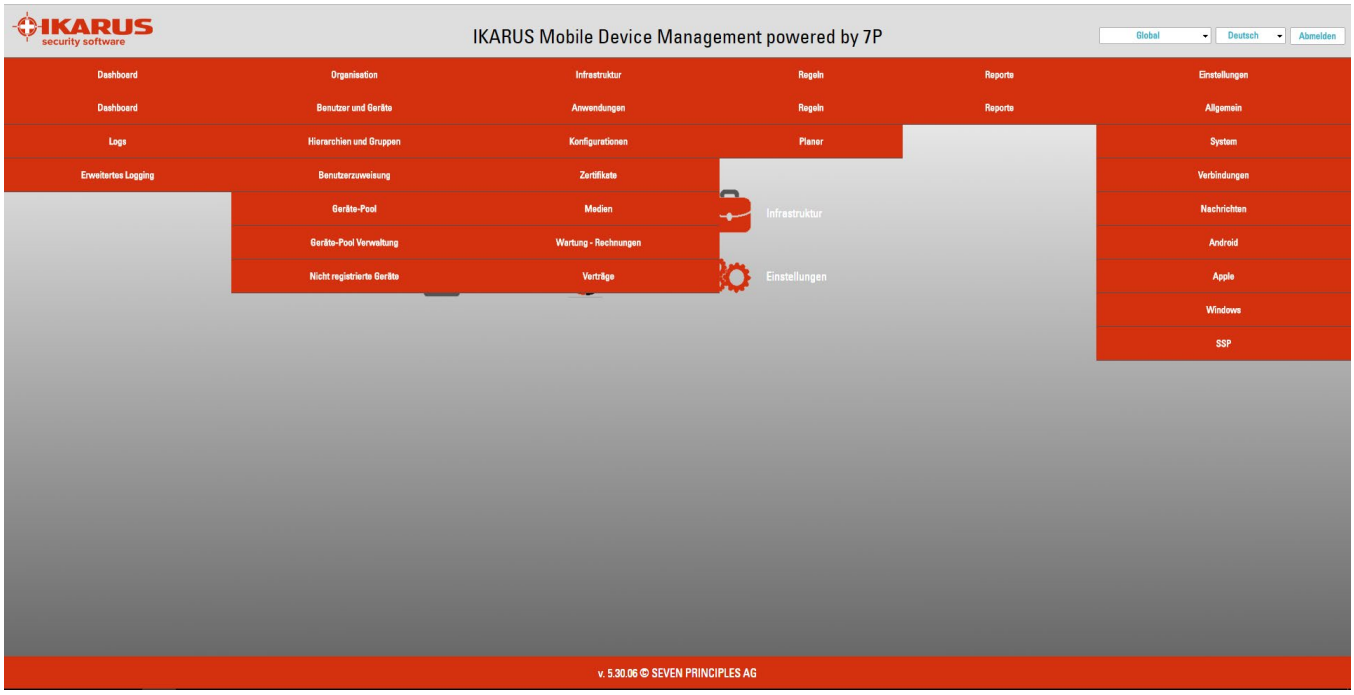


Abbildung 1: IKARUS mobile.management-Server 5.30.00 – globale Navigationsübersicht

Bei Auswahl eines Untermenüs wie beispielsweise „Dashboard“ öffnet sich das Dashboard-Steuerungsfenster.

4.3. Grundnavigation

Die Navigation durch die verschiedenen Hauptmenüpunkte, Untermenüs und Systemsteuerungen ist in diesem Dokument folgendermaßen zusammengefasst:

Mit der Navigation zu **System settings > Settings > Base >Tenants** *(Systemeinstellungen > Einstellungen > Basis > Mandanten)* wird der Administrator zum Konfigurationspanel „Mandanten“ innerhalb des IKARUS mobile.management-Servers geführt.

4.3.1. Befehlsnavigation

Die Befehlsnavigation besteht aus einem Befehl, der an die Navigationsanweisung angehängt ist: Durch Auswahl von **Organization > Hierarchies & groups > Add a new hierarchy** *(Organisation > Hierarchien & Gruppen > Neue Hierarchie hinzufügen)* wird der Administrator zum Befehl „Neue Hierarchie hinzufügen“ innerhalb des IKARUS-mobile.management-Servers geführt.

4.3.2. Home-Hyperlink

Auf jeder Seite links unten in der Fußzeile ist ein Hyperlink (^Home) eingefügt, der beim Anklicken den Leser zum Beginn des Dokuments zurückführt und nur im PDF-Format aktiv ist.

^Home

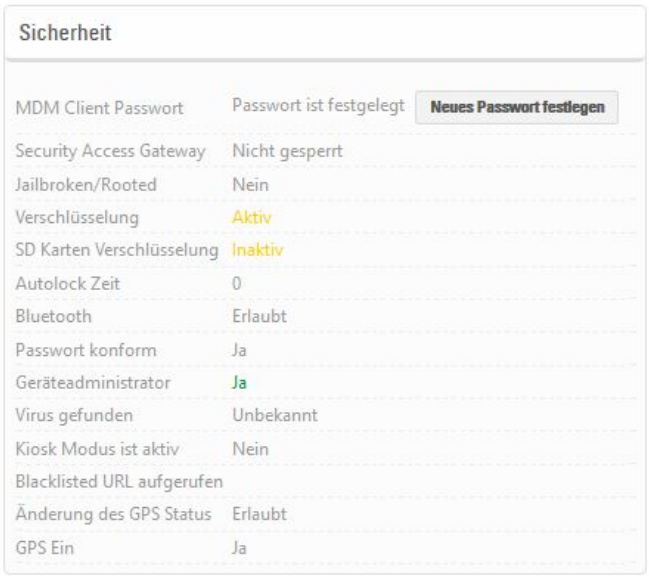
4.4. Menüpunkte

Das Größer-als-Zeichen (>) mit Leerstellen davor und danach trennt die Punkte im Menü.

Beispielsweise weist **Operations > Operations > Is roaming > Drop-down selection (Yes / No)** *(Abläufe > Abläufe > Roaming > Dropdown-Auswahl (Ja / Nein))* darauf hin, dass Sie zunächst „Operations“ *(„Abläufe“)* in den Hauptmenüregisterkarten wählen, dann „Operations“ *(„Abläufe“)* in den Menüoptionen auf der linken Seite, gefolgt von der Ablaufbezeichnung und schließlich der anzuwendenden Bedingung.

4.5. Farbige Statusanzeigen

Farbige Statusanzeigen sollen den Administrator unterstützen, indem ausgewählte Leistungsindikatoren (mit Hilfe von Farben) markiert werden, unabhängig davon, ob ein Status oder eine Metrik sich innerhalb oder außerhalb des gewünschten Bereichs befindet.



Aktuell sind auf dem IKARUS mobile.management-Server drei farbige Statusanzeigen vorhanden: Grün für ‚Alles OK‘, gelb für ‚Aufmerksamkeit erforderlich‘ und rot für ‚Warnung‘.

4.6. Allgemeine Fehlermeldungen

Fehlermeldungen sind grundsätzlich dazu gedacht, den Administrator darüber zu informieren, warum eine spezifische Funktion nicht ausgeführt wird, d. h. ob ein Datenkonflikt oder eine Typeninkongruenz besteht oder der gewünschte Parameter bereits verwendet wird.

^Home

Abbildung 2: Format Fehlermeldung

Fehlermeldungen enthalten möglichst exakte Informationen. Im Fall des obigen Datenkonflikts zeigt der IKARUS mobile.management-Server den Grund für den Fehler und liefert weitere Informationen, insbesondere Benutzer, Mandant und Gerätebezeichnung.

4.7. Auswahl Mandantenverhältnis und Sprache, Abmelden

Die Dropdown-Verzeichnisse für die Auswahl von Mandantenverhältnis und Sprache sind oben rechts auf der grafischen Benutzeroberfläche des IKARUS mobile.management-Servers angeordnet.

Durch Auswahl der Abmeldeschaltfläche wird der Benutzer abgemeldet.

4.8. Tooltip-Anzeige

Ein Pop-up-Fenster mit Informationen erscheint, wenn man mit der Maus über bestimmte komprimierte Informationsfelder fährt, so dass der Administrator das vollständige Informationsfeld beispielsweise in ein Notepad-Dokument kopieren und einfügen kann.

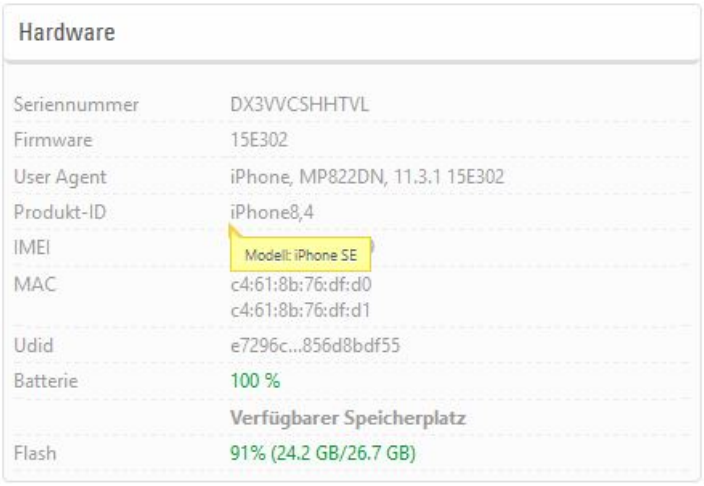
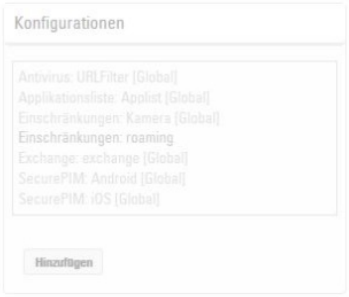


Abbildung 3: Tooltip-Feld aufgerufen durch Mouse-over

^Home

4.8.1. Grau dargestellte (schreibgeschützte) Elemente



Zwei unterschiedliche Farben werden verwendet, um auf schreibaktivierte (editierbare) sowie schreibgeschützte (nicht editierbare) Befehle und Informationen im gesamten IKARUS mobile.management-Server hinzuweisen.

- ✓ Schreibgeschützte Konfigurationselemente werden üblicherweise über die Sicherheitsmaßnahmen des Superadministrators konfiguriert (und geschützt).
- ✓ Schreibgeschützte Informationen können auch Informationen enthalten, die von einem Mobilgerät abgerufen werden und standardmäßig schreibgeschützt sind.
- ✓ Schreibgeschützte Informationen können auch absolute Werte, Informationen und Gesamtwerte enthalten, beispielsweise die in einem Bericht abgerufenen und angezeigten Informationen.

Alle Konfigurationsvorlagen, Anwendungen oder Parameter mit dem Suffix **[Global]** sind nur von einem Superadministrator editierbar. Bei allen Konfigurationsvorlagen, Administratorrollen oder Parametern wird die erstellende/erzeugende Bezeichnung des Mandantenverhältnisses eindeutig als Suffix in der globalen Mandantenansicht angezeigt, z.B. Zugriffspunkt [Dokumentation].

^Home

5. Administratoren, Benutzer und Gruppen

Der IKARUS mobile.management-Server ist vorkonfiguriert – entweder mit globalen Superadministratoren-Accounts oder einem definierten Mandantenverhältnis mit Mandaten-Accounts.

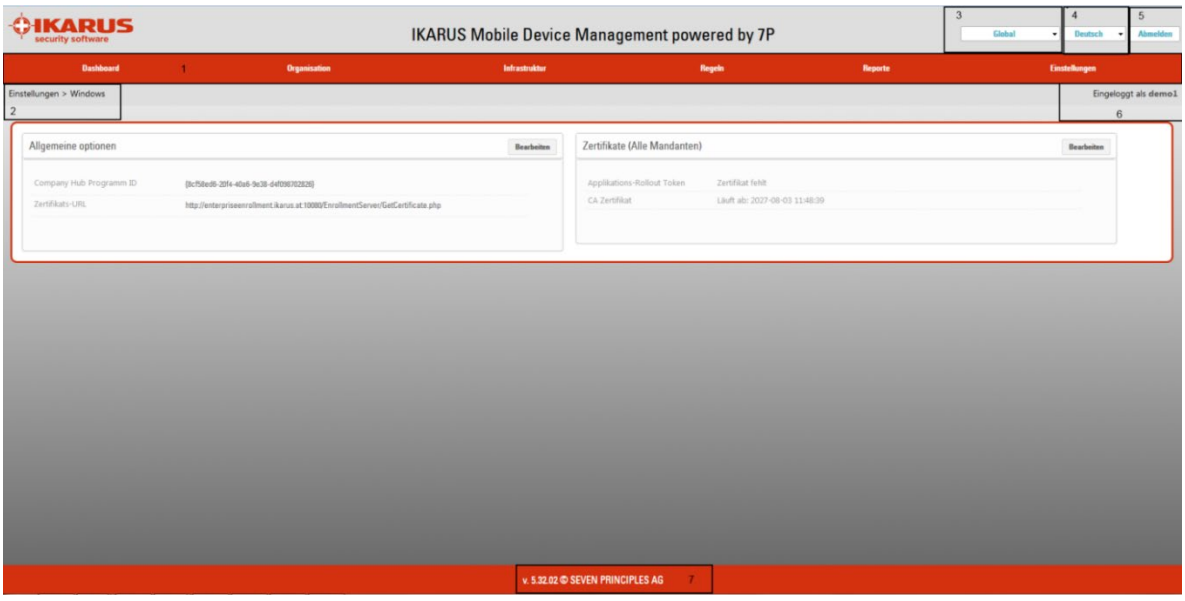
Typischerweise erhalten Sie eine Mitteilung mit der URL, dem Benutzernamen und dem Passwort des Mandantenadministrators für Ihr Mandantenverhältnis auf dem IKARUS mobile.management-Server.

> Das erste Mandantenadministrator-Passwort wird vom Anbieter des IKARUS mobile.management-Servers konfiguriert. Wenn Sie Schwierigkeiten haben, sich auf Ihrem Account anzumelden, dann kontaktieren Sie Ihren Anbieter, der Sie durch den Prozess führen wird.

Nach dem Anmelden besteht die Aufgabe für den Mandantenadministrator darin, weitere Administrator-Accounts zu erzeugen, eine Gruppenhierarchie zu definieren, die für Ihre Organisation geeignet ist, und Benutzer hinzuzufügen.

5.1. Erstanmeldung

Navigieren Sie nach der Erstanmeldung zu **Settings > Base** *(Einstellungen > Grundeinstellungen)*.



Die Benutzeroberfläche des IKARUS mobile.management-Servers besteht aus den folgenden Hauptelementen:

1. Hauptmenü-Navigationsleiste (durch Klicken auf die einzelnen Überschriften werden die Optionen des Dropdown-Untermenüs angezeigt)
2. Breadcrumb – die Stelle, an der Sie sich aktuell befinden
3. Bezeichnung des Mandantenverhältnisses
4. Sprachauswahl für die Benutzeroberfläche
5. Abmeldeschaltfläche
6. Detailangabe Benutzerauswahl

^Home

7. Version auf dem IKARUS mobile.management-Server

5.1.1. Weitere Administrator-Accounts erstellen

In diesem Beispiel verwenden wir ein Mandantenverhältnis mit dem Namen EMM01.

Navigieren Sie zu **Settings > Base > Admins** *(Einstellungen > Grundeinstellungen > Administratoren).*

Wählen Sie **Add new** *(Neu hinzufügen)* in der Administrator-Konfiguration (die Konfigurationsvorlage zum Hinzufügen neuer Administratoren wird angezeigt).

Geben Sie den Benutzernamen, das Passwort und die Wiederholung des Passworts in die vorgesehenen Felder ein.

Wählen Sie in der Rollen-Dropdown-Liste entweder den vorkonfigurierten Administrator, den Help-Desk-Administrator oder den Schreibschutz-Administrator.

Wählen Sie das Mandantenverhältnis (EMM01) im scrollbaren Mandantenverzeichnis.

Stellen Sie sicher, dass eine Firmen-E-Mail-Adresse im E-Mail-Feld eingefügt ist (wird für die Passwort-Wiederherstellung verwendet).

Wählen Sie schließlich Zwei-Faktor-Authentifizierung **– Off** *(Aus)*.

Wählen Sie **OK**.

Der neue Administrator-Account wird definiert und die Administratorrollen werden erstellt.

Logout vom IKARUS mobile.management-Server. Melden Sie sich mit dem neu erstellten Administrator-Account an.

Login auf dem IKARUS mobile.management-Server mit dem neu erstellten Administrator-Benutzernamen und -Passwort. Sie werden in das Mandantenverhältnis EMM01 eingeloggt.

5.2. Hierarchien und Gruppen erstellen

Hierarchien und Gruppen ermöglichen es dem Administrator des IKARUS mobile.management-Systems, eine Organisationsstruktur mit logischen Ebenen entweder zur Darstellung der eigenen Organisationsstruktur oder zur Erstellung einer neuen Organisationsstruktur zu definieren oder eine neue Organisationsstruktur zur Unterstützung des Mobilgerätemanagements zu erstellen.

^Home

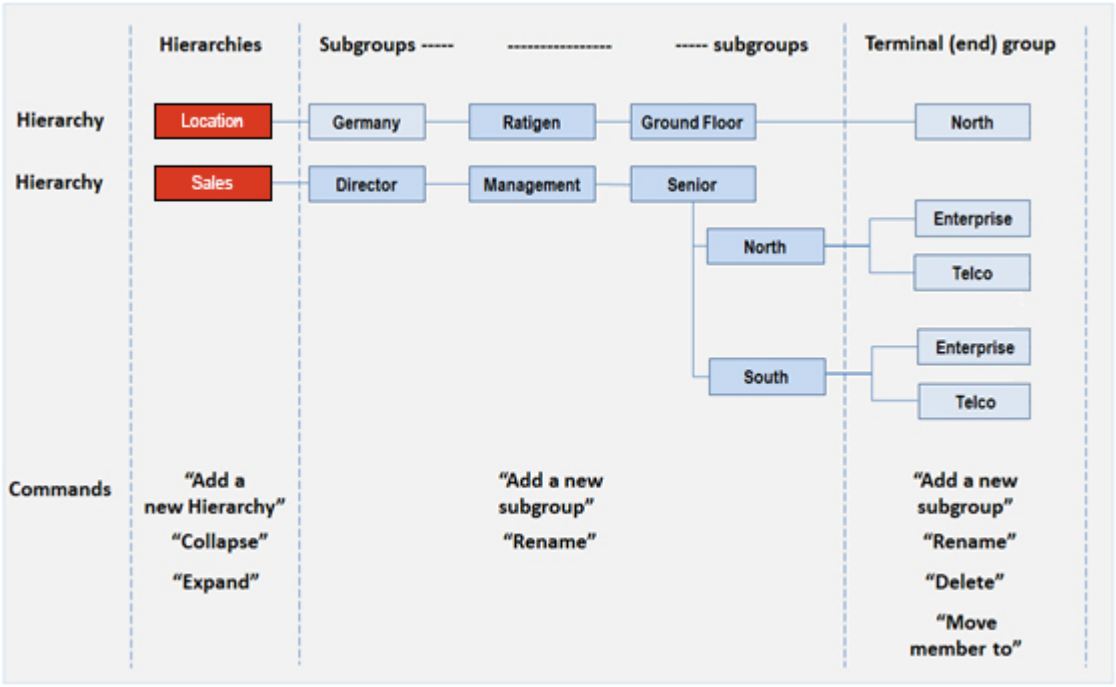


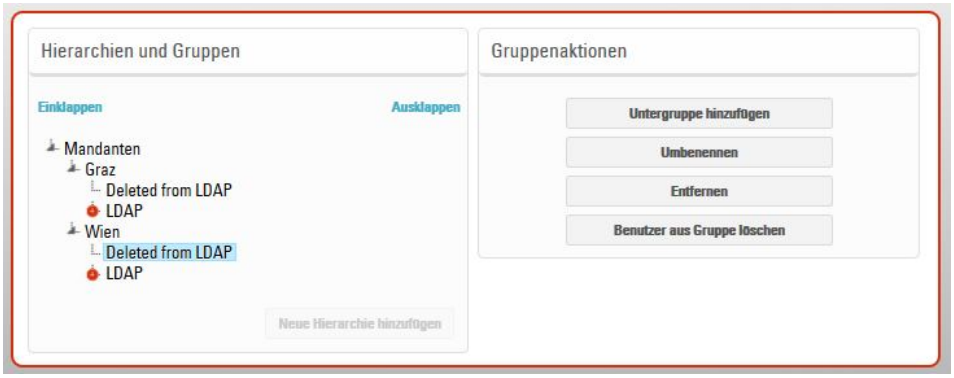
Abbildung 4: Zusammenfassung Hierarchie- und Gruppenbefehle

5.2.1. Eine einfache Gruppenhierarchie erstellen

Navigieren Sie zu **Organization > Hierarchy & Groups** *(Organisation > Hierarchie & Gruppen)*

Wählen Sie **Add new hierarchy** *(Neue Hierarchie hinzufügen)* und geben Sie „Sales"*(Vertrieb)* im angezeigten Pop-up-Fenster ein. „Sales" wird dann in der Hierarchie erscheinen.

Wählen Sie **Add new hierarchy** *(Neue Hierarchie hinzufügen)* und geben Sie „North" *(Nord)* im angezeigten Pop-up-Fenster ein. „North" wird dann in der „Sales"-Hierarchie erscheinen.



Wählen Sie erneut **Sales**, dann wählen Sie **Add a new subgroup** *(Neue Untergruppe hinzufügen)* und geben Sie „South" *(Süd)* im angezeigten Pop-up-Fenster ein. „South" wird dann in der „Sales"-Hierarchie erscheinen.

^Home

5.3. Einen neuen Benutzer hinzufügen

Navigieren Sie zu **Organization > Users and devices > Add user** *(Organisation > Benutzer und Geräte > Benutzer hinzufügen).*

Vorname, Nachname und entweder E-Mail-Adresse **ODER** Benutzer-ID sind **Pflichtfelder**, die beim Hinzufügen eines neuen Benutzers ausgefüllt werden müssen.

Felder mit Benutzerinformationen:

Angabe	Beschreibung
Vorname*	Vorname des neuen Benutzers
Nachname*	Nachname des neuen Benutzers
E-Mail-Adresse*	Eine E-Mail-Adresse des neuen Nutzers (**verbindlich** ist entweder die E-Mail-Adresse ODER die Benutzer-ID)
Benutzer-ID*	Ein eindeutiger Zahlencode, der dem Benutzer manuell zugewiesen wird (**verbindlich** ist entweder die E-Mail-Adresse ODER die Benutzer-ID)
WINDOWS-Benutzername	Wenn es sich um einen WINDOWS-Benutzer handelt, ist ein WINDOWS-Benutzername erforderlich.
Passwort	Wenn es sich um einen WINDOWS-Benutzer handelt, ist ein Passwort erforderlich.
Zugewiesene Mobilnummer	Die MSISDN-Nummer der SIM-Karte, die dem Benutzer vom Administrator zugewiesen wird („Multiuser“ muss aktiviert sein)
Gruppenzuweisung	Die Gruppen, in denen der neue Benutzer Mitglied sein wird
Individuelle Parameter	Dem Benutzer zugewiesene individuelle Parameter, wobei diese Werte von den Benutzergeräten übernommen werden.

Tabelle 1: Benutzerangaben

Nach Fertigstellung der Bearbeitung muss der Administrator **Save** *(Speichern)* wählen, um die Benutzerdaten für den IKARUS mobile.management-Server zu aktualisieren.

5.3.1. Benutzer löschen

Navigieren Sie zu **Organization > Users and devices > Username** *(Organisation > Benutzer und Geräte > Benutzername).*

Wählen Sie **Delete** *(Löschen)* im Fenster mit den Benutzerangaben.

^Home

Alle dazugehörigen Daten, einschließlich Geräte, Anwendungen, installierte Konfigurationen und Historie werden dann vom IKARUS mobile.management-Server gelöscht.

5.4. Mehrere Benutzer über einen CSV-Import hinzufügen

Das Dienstprogramm für den CSV-Import ermöglicht es dem Administrator, einen bis hin zu mehreren tausend Benutzern zu importieren, indem er über die „CSV-Import"-Funktion des IKARUS mobile.management-Servers eine valide CSV-Datei übermittelt.

Unten sehen Sie beispielhaft eine einfache CSV-Datei, die „Saved as CSV" *(gespeichert als CSV)* von Microsoft Excel exportiert wurde, wobei das Komma als CSV-Trennzeichen ausgewählt wurde. Bei den Spaltenüberschriften ist die Groß- und Kleinschreibung zu beachten.

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

Navigieren Sie zu **Organization > Users and devices** *(Organisation > Benutzer und Geräte),* dann wählen Sie die Schaltfläche **CSV import**. Das CSV-Import-Fenster erscheint.

Die Schaltfläche **Choose File** *(Datei auswählen)* erlaubt dem Administrator, das Dateisystem auf die vorbereitete CSV-Datei zu durchsuchen. Nach der Auswahl wird der Name der CSV-Datei neben der Schaltfläche **Choose File** *(Datei auswählen)* angezeigt.

Durch Auswahl der Schaltfläche „Import" auf dem CSV-Fenster wird die CSV-Importfunktion angestoßen.

Die Zeit, die für den Import von Benutzerinformationen von einer vorbereiteten CSV-Datei nötig ist, hängt von der Anzahl an Datensätzen in der CSV-Datei ab. Nach Fertigstellung des CSV-Imports werden die Benutzer für das Hinzufügen von Geräten verfügbar sein.

Wenn die Benutzer-ID als bevorzugte (verbindliche) Identifikationsmethode verwendet wird (siehe **Settings > Base> Common options (all tenants) > User identification** *(Einstellungen > Grundeinstellungen > Gemeinsame Optionen (alle Mandanten) > Benutzeridentifikation)*), dann ersetzen Sie die CSV-Überschrift „email" mit der Benutzer-ID („userID").

^Home

6. Hinzufügen eines einfachen Android-Gerätes

Der IKARUS mobile.management-Server verlangt die Installation und Authentifizierung der Android-Anwendung des IKARUS mobile.management-Clients auf dem physischen Gerät, bevor das Gerätemanagement beginnen kann. Dieser Prozess wird als Geräteanmeldung bezeichnet. Der Geräteanmeldungsprozess unterscheidet sich bei Android Enterprise, Samsung KNOX, Samsung KME und einfachen Android-Geräten geringfügig.

Ein einfaches (allgemeines) Android-Gerät verwendet normalerweise die Google-Android-API-Funktion.

- ✓ Bei Mobiltelefonen beginnt die Geräteanmeldung, wenn der Benutzer eine SMS-Textnachricht öffnet, die vom Administrator des IKARUS mobile.management-Servers an das Gerät geschickt wurde.
- ✓ Bei Wifi-Geräten beginnt die Geräteanmeldung, wenn der Benutzer eine E-Mail-Nachricht öffnet, die vom Benutzer des IKARUS mobile.management-Servers an das Gerät geschickt wurde.

6.1. SMS-Anmeldung eines einfachen Android-SIM-Geräts

Navigieren Sie zu **Organization > Users and devices > Designated_User > Add device** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > Gerät hinzufügen).* Das Fenster zur Datenkonfiguration des neuen Geräts wird angezeigt und der Benutzer muss darin die Registerkarte **Android** wählen. (Weitere Angaben zur Android-Konfiguration werden nach der Auswahl angezeigt.)

Geben Sie einen benutzerfreundlichen Namen in des Namensfeld des Geräts sowie eine gültige Mobiltelefonnummer (unter Verwendung des internationalen Formats, z.B. +43) ein.

Nachdem die Mobiltelefonnummer eingegeben wurde, wird die Schaltfläche „Enroll via SMS“ *(Über SMS anmelden)* unten im Fenster für die Konfiguration der neuen Gerätedaten aktiv.

Wählen Sie **Enroll via SMS** *(Über SMS anmelden).*

Eine SMS-Textnachricht wird an die bereitgestellte Telefonnummer gesendet. Die SMS-Nachricht enthält den Download-Link für die IKARUS mobile.management-Client-Anwendung, die auf dem Gerät des Benutzers installiert werden muss. In die SMS-Textnachricht ist ein verschlüsselter Aktivierungscode integriert, der von der IKARUS mobile.management-Client-Anwendung für die Authentifizierung und die Kommunikation mit dem IKARUS mobile.management-Server verwendet wird.

Nach Empfang der Textnachricht gilt für den Benutzer:

- ✓ Er muss die Textnachricht öffnen und die Hyperlink-URL antippen/auswählen. Nach Auswahl des Hyperlinks wird der IKARUS mobile.management-Client automatisch auf das Gerät heruntergeladen.
- ✓ Er erhält möglicherweise eine Warnung, dass das Gerät keine Anwendungen von unbekannten Quellen installieren wird, und dem Anwendungsmanager kann ein interner Link präsentiert werden.
- ✓ Er muss die Installation von Anwendungen von unbekannten Quellen ermöglichen.

^Home

Während der Installation wird der Benutzer möglicherweise von der Anwendung gebeten, Standardgenehmigungen, Bedingungen und Lizenzierungsanforderungen zu akzeptieren. Der Benutzer muss als Teil des Installationsprozesses alle Anforderungen akzeptieren.

Wenn die IKARUS mobile.management-Client-Anwendung auf dem Gerät installiert wurde, wird sie sich automatisch gegenüber dem IKARUS mobile.management-Server identifizieren. Der IKARUS mobile.management-Client zeigt an, dass er **aktiviert** ist, wenn die Authentifizierung gegenüber dem IKARUS mobile.management-Server abgeschlossen ist.

Der IKARUS mobile.management-Administrator kann nun die (zurück übermittelten) Geräteangaben anzeigen, die vom IKARUS mobile.management-Client an den IKARUS mobile.management-Server gesendet wurden.

Navigieren Sie zu **Organization > Users and devices > Designated_User > Newly_added_ device** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > Neu hinzugefügtes Gerät).*

Prüfen Sie Bestand, Detailangaben, Aktionen, Historie, Installationen sowie SIM-Karten-Fenster.

6.2. E-Mail-Anmeldung eines einfachen Android-Wifi-Geräts

Die E-Mail-Anmeldung wurde für Wifi-Geräte konzipiert. Das anmeldende Gerät muss in der Lage sein, einen in der Anmeldungs-E-Mail angezeigten QR-Code zu scannen. Es empfiehlt sich, dass der Empfänger die Anmeldungs-E-Mail auf dem Laptop oder der Workstation dann öffnet, wenn sich das anzumeldende Wifi-Gerät in der Nähe befindet.

Navigieren Sie zu **Organization > Users and devices > Designated_User > Add device** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > Gerät hinzufügen).* Das Fenster zur Datenkonfiguration des neuen Geräts wird angezeigt und der Benutzer muss darin die Registerkarte **Android** wählen. (Weitere Angaben zur Android-Konfiguration werden nach der Auswahl angezeigt.)

Geben Sie im Feld für den Gerätenamen einen benutzerfreundlichen Namen ein. Es sind keine anderen Informationen erforderlich.

Diese E-Mail wird an die Unternehmens-E-Mail-Adressen der registrierten Benutzer gesendet, die in **Organization > Users and devices > Designated_User > Email** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > E-Mail)* registriert sind.

Wählen Sie unten im Konfigurationsfenster für neue Gerätedaten **Enroll via email** *(Über E-Mail anmelden)*.

Der benannte Benutzer erhält eine E-Mail, die den Download-Link für die IKARUS mobile.management-Client-Anwendung enthält.

Nach Empfang der E-Mail-Nachricht gilt für den Benutzer:

- ✓ Er muss die E-Mail auf dem Gerät öffnen und die Hyperlink-URL antippen/auswählen. Nach Auswahl des Hyperlinks wird der IKARUS mobile.management-Client automatisch auf das Gerät heruntergeladen.

^Home

- ✓ Er muss zudem die E-Mail auf einem anderen Gerät (z.B. Laptop, Workstation oder auch ein anderes Mobilgerät) öffnen, so dass der in der Anmeldungs-E-Mail integrierte QR-Code angezeigt werden kann.
- ✓ Er erhält möglicherweise eine Warnung, dass das Gerät keine Anwendungen von unbekannten Quellen installieren wird, und dem Anwendungsmanager kann ein interner Link präsentiert werden.
- ✓ Er muss die Installation von Anwendungen von unbekannten Quellen ermöglichen.

Der IKARUS mobile.management-Client wird installiert.

Während der Installation erscheint der Aktivierungsbildschirm. Der Benutzer muss „Activate with QR code" *(Mit QR-Code aktivieren)* auswählen und den QR-Code, den er in der Anmeldungs-E-Mail erhielt, über die IKARUS mobile.management-Client-Anwendung scannen.

Der Benutzer wird dann gebeten, einen Sicherheitscode vorzulegen, der typischerweise 1234 ist.

Während der Installation wird der Benutzer möglicherweise von der Anwendung gebeten, Standardgenehmigungen, Bedingungen und Lizenzierungsanforderungen zu akzeptieren. Der Benutzer muss als Teil des Installationsprozesses alle Anforderungen akzeptieren.

Wenn die IKARUS mobile.management-Client-Anwendung auf dem Gerät installiert wurde, wird sie sich automatisch gegenüber dem IKARUS mobile.management-Server identifizieren. Der IKARUS mobile.management-Client zeigt an, dass er **aktiviert** ist, wenn die Authentifizierung gegenüber dem IKARUS mobile.management-Server abgeschlossen ist.

Der IKARUS mobile.management-Administrator kann nun die (zurück übermittelten) Geräteangaben anzeigen, die vom IKARUS mobile.management-Client an den IKARUS mobile.management-Server gesendet wurden.

Navigieren Sie zu **Organization > Users and devices > Designated_User > Newly_added_ device** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > Neu hinzugefügtes Gerät).*

Prüfen Sie Bestand, Detailangaben, Aktionen, Historie, Installationen sowie SIM-Karten-Fenster.

7. Ein iOS-Gerät hinzufügen

Wenn ein Systemadministrator ein iOS-Gerät zum IKARUS mobile.management Server hinzufügt, dann wird eine E-Mail (oder SMS-Textnachricht bei einem SIM-aktivierten Gerät) erzeugt, die eine Hyperlink-URL enthält, die bei Öffnen auf dem iOS-Gerät des Benutzers das iOS-Gerät in der Installation des Apple-IKARUS mobile.management Profils instruieren wird. Wenn das Apple-IKARUS mobile.management-Profil installiert ist, muss der IKARUS mobile.management-Client zum Gerät hinzugefügt werden.

^Home

7.1. Hinzufügen eines iOS-SIM-Geräts

Navigieren Sie zu **Organization > Users and devices > Designated_User > Add device** (Organisation > Benutzer und Geräte > Bezeichnete Benutzer > Gerät hinzufügen).

Das Fenster zur Datenkonfiguration des neuen Geräts wird angezeigt und der Benutzer muss darin die Registerkarte **iOS** wählen.

Geben Sie einen benutzerfreundlichen Namen in des Namensfeld des Geräts sowie eine gültige Mobiltelefonnummer (unter Verwendung des internationalen Formats, z.B. +43) ein.

Nachdem die Mobiltelefonnummer eingegeben wurde, wird die Schaltfläche „Enroll via SMS" (Anmelden über SMS) unten im Fenster für die Konfiguration der neuen Gerätedaten aktiv.

Wählen Sie **Enroll via SMS** (Anmelden über SMS).

Eine SMS-Textnachricht, die den iOS-Profil-Hyperlink enthält, wird an das Gerät gesendet. Der Benutzer wählt dann den Hyperlink innerhalb der SMS-Textnachricht.

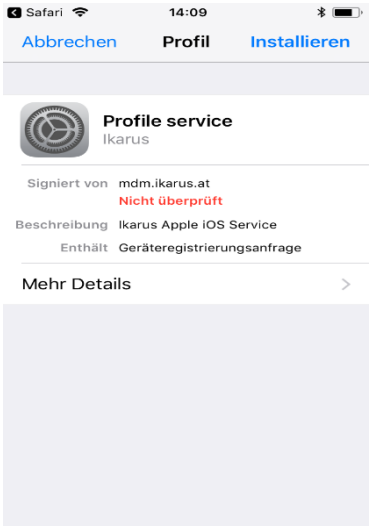


Abbildung 5: URL-Link für den Profilprozess geöffnet

Eine neue Webseite öffnet sich auf dem Benutzergerät. Der Benutzer kann entweder das IKARUS mobile.management-Profil installieren oder den Vorgang abbrechen. Der Benutzer wird nach dem Gerätepasswort gefragt. Auf die korrekte Eingabe des Gerätepassworts hin wird das IKARUS mobile.management-Profil installiert.

Der IKARUS mobile.management-Administrator kann nun die (zurück übermittelten) Geräteangaben anzeigen, die vom IKARUS mobile.management-Profil an den IKARUS mobile.management-Server gesendet wurden.

Navigieren Sie zu **Organization > Users and devices > Designated_User > Newly_added_ device** *(Organisation > Benutzer und Geräte > Bezeichneter Benutzer > Neu hinzugefügtes Gerät).*

^Home

Prüfen Sie Bestand, Detailangaben, Aktionen, Historie, Installationen sowie SIM-Karten-Fenster.

8. Android-Enterprise-Funktion hinzufügen

„Android for Enterprise“ ist eine kostenlose Funktion von Google, die in vielen Mobilgeräten mit Android als Mobilbetriebssystem verwendet werden kann. Diese Funktion ermöglicht es Ihnen, ein sogenanntes Arbeitsprofil zu aktivieren, mit dem private Daten und Unternehmensdaten getrennt werden können. Informationen zu aktuell unterstützten Geräten finden Sie am Ende dieses Kapitels.

8.1. Anforderungen

Ein Gmail-Account ist erforderlich, um Ihre IKARUS mobile.management-Serverinstanz in „Android for Enterprise“ anzumelden (globale Instanz oder Mandanteninstanz). Wenn Sie keines haben, dann erstellen Sie einen allgemeinen Account (basierend auf Ihrem Unternehmen), auf das die autorisierten IT-Administratoren in Ihrem Unternehmen zugreifen können. Beispielsweise könnten Sie Ihre(n) Firmennamen mit einem AfE-Suffix (für "Android for Enterprise") verwenden. Private (persönliche) Accounts sollten nicht verwendet werden.

8.2. Vorbereitung

Bevor Sie „Android for Enterprise“ auf Ihren Mobilgeräten starten können, überlegen Sie, ob Ihre KARUS mobile.management-Installation „Android for Enterprise“ global eingesetzt werden soll, so dass alle Mandanten einen „Android for Enterprise“-Account verwenden können, oder durch mehrere Einzelmandanten, wobei jeder Mandant einen eigenen „Android for Enterprise“-Account anmelden muss.

8.2.1. Globale Mandantenprüfung

1. Melden Sie sich auf dem IKARUS mobile.management-Server an.
2. Stellen Sie sicher, dass aktuell das Mandantenverhältnis „Global“ angezeigt wird.
3. Navigieren Sie zu **Settings > Android > Android Enterprise** *(Einstellungen > Android > Android Enterprise)* und stellen Sie sicher, dass das Authentifizierungssymbol für den Enterprise-Anmeldungsdienst und eine sichtbare Datei (ermöglicht die Kommunikation zwischen dem IKARUS mobile.management-Server und Googles Enterprise) vorhanden sind.

Bitte kontaktieren Sie IKARUS, wenn kein Authentifizierungssymbol für den Anmeldungsdienst angezeigt wird.

8.2.2. Mandantenprüfung

1. Melden Sie sich auf dem IKARUS mobile.management-Server an.
2. Stellen Sie sicher, dass aktuell das korrekte Mandantenverhältnis angezeigt wird.
3. Navigieren Sie zu **Settings > Android > Android Enterprise** *(Einstellungen > Android > Android Enterprise)* und stellen Sie sicher, dass im Unternehmens-ID-Feld ein Fertigstellungssymbol angezeigt wird.

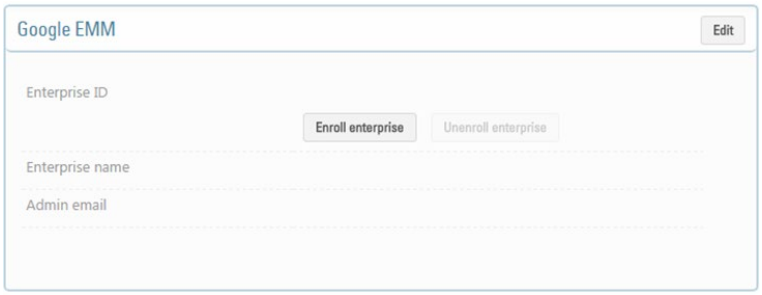
^Home

Bitte kontaktieren Sie IKARUS, wenn kein Fertigstellungssymbol angezeigt wird.

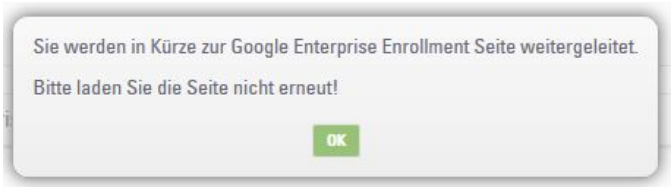
8.3. Unternehmen anmelden

Die Anmeldeprozesse für einen globalen Mandanten und einen Kundenmandanten sind gleich:

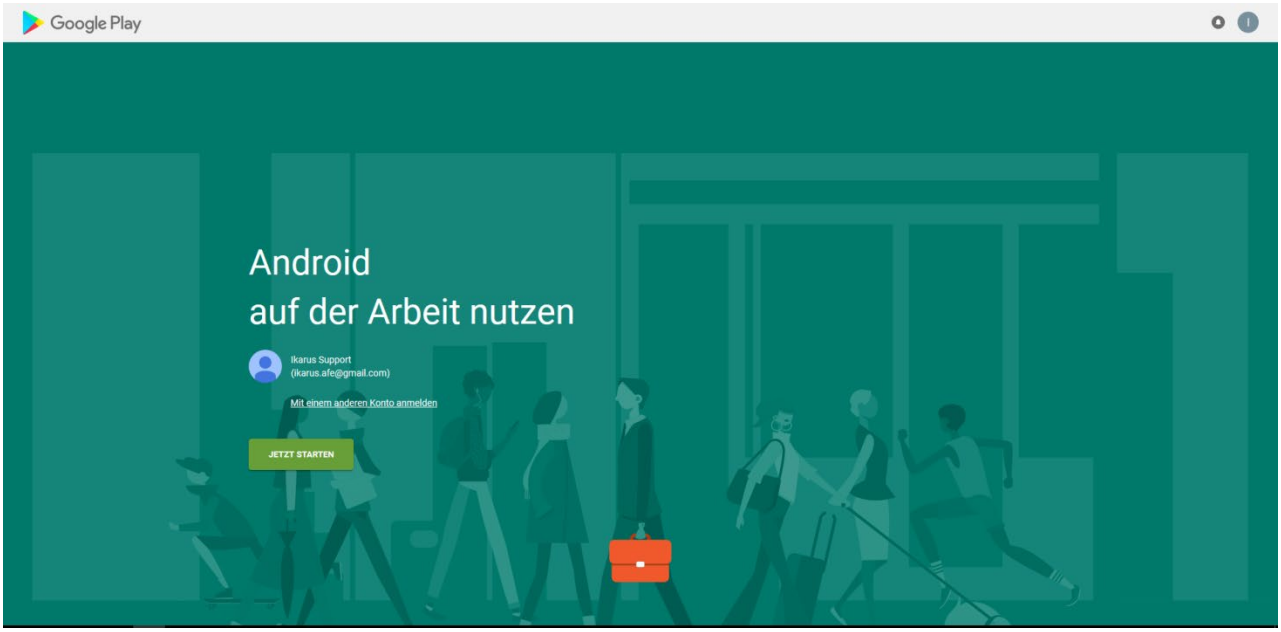
1. Navigieren Sie zu **Settings > Android > Android Enterprise** *(Einstellungen > Android > Android Enterprise)* und wählen Sie die Schaltfläche **Enroll enterprise** *(Unternehmen anmelden).*



2. Das folgende Feld wird kurz angezeigt und Sie werden zu Google umgeleitet – wählen Sie OK.



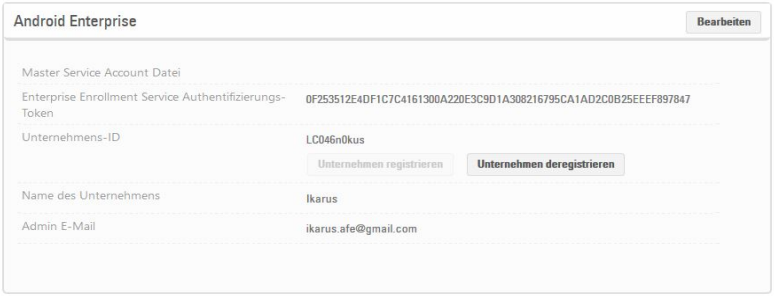
Nach der Auswahl erscheint die folgende Google-Schnittstelle. Stellen Sie sicher, dass der korrekte Google-Account verwendet wird, bevor Sie beginnen.



^Home

Wenn ein alternativer Account zugewiesen wurde, dann wählen Sie „Sign in with a different account" *(Anmelden mit einem anderen Account)* – geben Sie den Benutzernamen und das Passwort ein.

Nach einigen Sekunden werden Sie automatisch zum IKARUS mobile.management-System umgeleitet und weitere Informationen werden im Android-Enterprise-Fenster angezeigt.



Der Google-EMM-Registrierungsbildschirm enthält folgende Anzeigen bei IKARUS mobile.management:

Unternehmens-ID – von der Google-Infrastruktur zurück übermittelt

Unternehmensname – der Name, der zur Anmeldung des Unternehmens verwendet wurde

Admin-E-Mail – E-Mail-Adresse des anmeldenden Accounts

Die Auswahl von „Unenroll enterprise" (Unternehmen abmelden) führt zur Trennung aller Account-Daten, Anschaffungen und Bereitstellungen vom IKARUS mobile.management-Server. Diese Account-Daten mit allen ausstehenden Beträgen werden nach wie vor von dem Account bezahlt, das zur Anmeldung des Unternehmens verwendet wurde.

Damit sind alle Vorbereitungen abgeschlossen und Sie können mit dem Einsatz des Geräts beginnen.

8.4. Einsatz des Geräts

Für diesen Abschnitt wird davon ausgegangen, dass der IKARUS mobile.management-Client 5.27.02 oder höher in ein Gerät mit *Arbeitsprofil*-Fähigkeit installiert wurde, sich in einer Online-Verbindung mit dem IKARUS mobile.management-Server befindet, aktiviert ist und einen gültigen Datenanschluss hat.

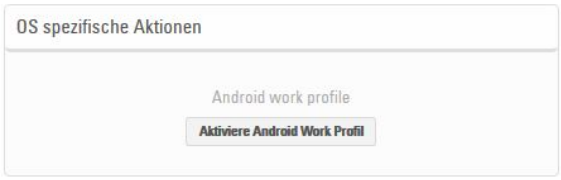
Um das Android Enterprise Profile (Arbeitsprofil) auf Android-Geräten zu aktivieren, führen Sie bitte folgende Aktionen durch:

1. Melden Sie das Gerät wie gewöhnlich durch Installieren und Aktivieren des IKARUS mobile.management-Clients auf dem Gerät an.

^Home

Bei erfolgreichem Abschluss der Geräteanmeldung führen Sie folgende Aktionen durch:

2. Navigieren Sie zu **Organization > Users and devices > User > Device> Actions > OS specific actions** (Organisation > Benutzer und Geräte > Benutzer > Gerät > Aktionen > OS-spezifische Aktionen).
3. Wählen Sie die Schaltfläche „Activate Android Work Profile“ (Android-Arbeitsprofil aktivieren).

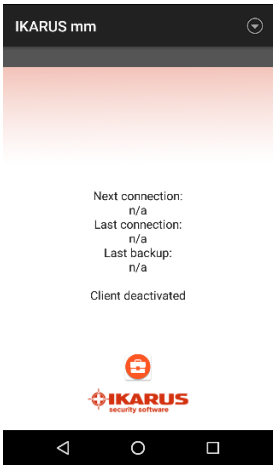


4. Der Eintrag eines zusätzlichen Geräts (Arbeitsprofil) in die Liste wird automatisch für das ausgewählte Gerät erstellt.

Das Symbol für das Android-Arbeitsprofil (Aktenkoffer) erscheint auf der Benachrichtigungsleiste des Geräts, die die Benachrichtigung des IKARUS mobile.management-Servers anzeigt, wenn sie heruntergezogen wird.

5. Bei der nächsten Geräteverbindung beginnt die Aktivierung des Geräts (Arbeitsprofils).
   a. Akzeptieren Sie die Geschäftsbedingungen.
   b. Bestätigen Sie die Einrichtung des Arbeitsprofils.
   c. Neuere Geräte sind standardmäßig bereits verschlüsselt. Andere Geräte, die das Gerät (Arbeitsprofil) unterstützen, werden als Teil der Geräteinitialisierung (Arbeitsprofil) verschlüsselt. Ohne Geräteverschlüsselung kann das Arbeitsprofil nicht aktiviert werden.
   d. Nach erfolgreicher Verschlüsselung (falls erforderlich), startet das Gerät neu und die Aktivierung des Arbeitsprofils wird fortgesetzt. Wenn dieser Prozess nicht automatisch startet, prüfen Sie auch die Benachrichtigungen in der Benachrichtigungsleiste (oben am Bildschirm).
   e. Das Arbeitsprofil wird nun eingerichtet und ein dedizierter IKARUS mobile.management-Client wird für dieses Profil wird aktiviert.

^Home



IKARUS mobile.management-Arbeitsprofil-Client beginnt mit der Aktivierung.

IKARUS mobile.management-Arbeitsprofil-Client ist aktiviert.

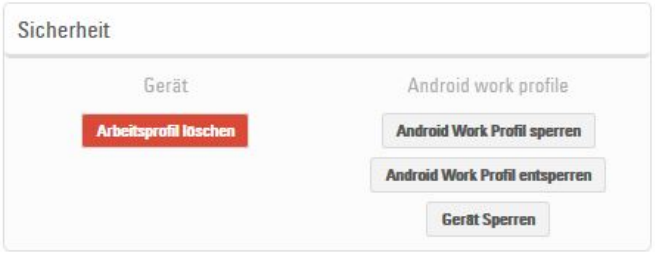
f. Nach erfolgreicher Aktivierung des Arbeitsprofil-Client wird ein Aktenkoffer-Symbol auf dem IKARUS mobile.management-Client angezeigt. Alle Anwendungen innerhalb des Geräts (Arbeitsprofil) zeigen auch das Aktenkoffersymbol auf ihrem Anwendungssymbol an.

g. Auf der IKARUS mobile.management-Benutzeroberfläche können Sie zudem sehen, dass der IKARUS mobile.management-Client für das Arbeitsprofil aktiviert ist.

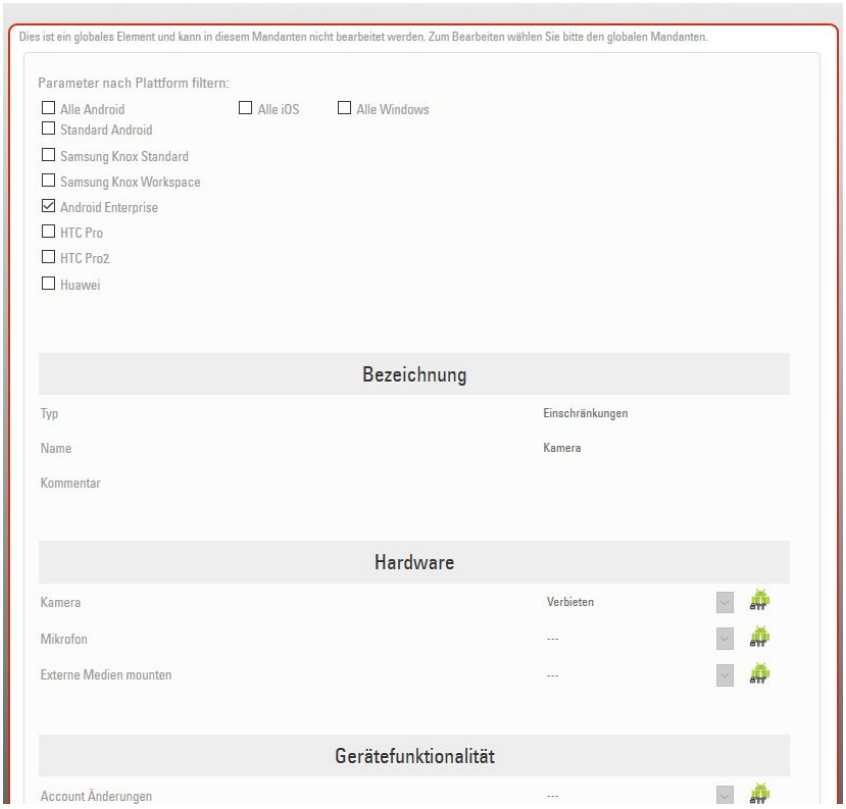
Dieser Eintrag gilt als unabhängiges (virtuelles) Gerät und kann unabhängig vom aktuellen physischen Gerät verwaltet werden. Deshalb erhält es einen eigenen Bestands- und Administrationsbereich.

Navigieren Sie zu **Organization > Users and devices > User > Device (work profile)> Actions > Security** *(Organisation > Benutzer und Geräte > Benutzer > Gerät (Arbeitsprofil) > Aktionen > Sicherheit).*

^Home



Mit diesem Symbol werden die Konfigurationsparameter, die für das Arbeitsprofil „Android for Enterprise“ unterstützt werden, markiert.



Daher können Sie individuelle Konfigurationsvorlagen für Ihre „Android for Enterprise“-Arbeitsprofile erstellen.

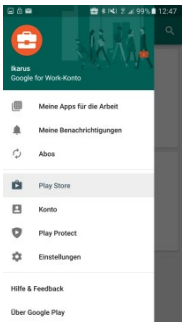
8.5. Offizielles Geräteverzeichnis

Für eine aktuelle Version von „Android for Enterprise“-kompatiblen Geräten besuchen Sie https://www.android.com/enterprise/devices/.

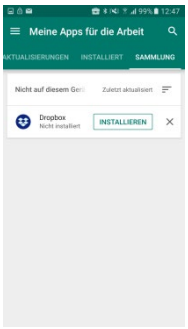
9. (Individueller) Layout-Editor für Managed Google Play Store

Der Play Store (Arbeitsprofil) enthält zwei separate Anwendungspositionen.

^Home



Store Home



My work apps

Abbildung 6: Account-Anzeige Play Store (Arbeitsprofil) des Geräts

Der (individuelle) Layout-Editor für den Managed Google Play Store des IKARUS mobile.management-Servers ermöglicht es dem Administrator, auf dem Benutzergerät die verfügbaren genehmigten Arbeitsprofilanwendungen organisiert und benutzerdefiniert zu präsentieren.

Der erste Layout-Editor für den verwalteten Google Play Store hat eine Standardseite, nämlich Seite 1, ohne aufgelistete Anwendungen.

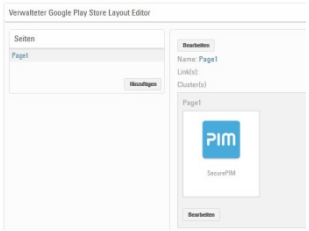


Abbildung 7: Standard (wie ausgeliefert)

Der Editor des verwalteten Google Play Store ist eine optionale Komponente des IKARUS mobile.management-Servers, für den entweder der globale Umfang des IKARUS mobile.management-Servers oder der aktuelle Mandantenumfang (Mandantenverhältnis des Administrators) des IKARUS mobile.management-Servers erforderlich ist, so dass ein angemeldetes Google-EMM-Unternehmen vorhanden ist, bevor der verwaltete Google Play Store verfügbar wird.

Abbildung 8: Registerkarte (individueller) Layout-Editor Google Play Store

^Home

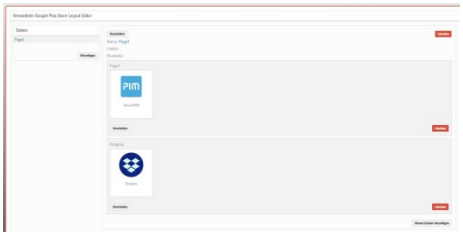
Ein Account mit globalem Umfang oder ein Google-EMM-Enterprise-Account mit Mandantenverhältnis muss vorhanden sein, bevor der Layout-Editor für den Managed Google Play Store Informationen aus dem Managed Google Play Store abrufen und anzeigen kann.

9.1. Verwendung des (individuellen) Layout-Editors für Managed Google Play Store

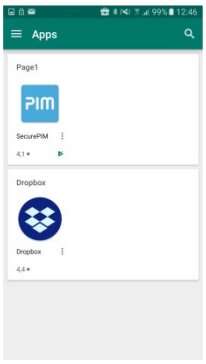
Der standardmäßige Layout-Editor für den verwalteten Play Store zeigt eine Seite mit der Bezeichnung „Seite 1", die nicht gelöscht werden kann. Der Seitenname kann jedoch bearbeitet werden. Der Layout-Editor besteht aus:

- ✓ Seiten – zur Unterstützung der logischen Organisation von Anwendungen
  - Seiten hinzufügen – Diese Seiten können zu jedem Zeitpunkt umbenannt werden.
  - Seiten löschen – Löschen irgendeiner Seite (außer der Standardseite Seite 1) – Alle Cluster- und Anwendungslink-Daten werden gelöscht. Die Anwendungen werden nicht gelöscht.
  - Seitentitel umbenennen – Nach dem Umbenennen der Seite bleiben die Apps in der bearbeiteten Seite vorhanden.
  - Nur Seiten können Links zu anderen Seiten enthalten.
- ✓ Links (zu anderen Seiten)
  - Links zu den erstellten Seiten hinzufügen (außer auf die eigene Seite)
  - Links zu anderen erstellten Seiten löschen
- ✓ Cluster (logische Gruppierung von Anwendungen)
  - Die Seiten können einen oder mehrere Cluster enthalten.
  - Jedes Cluster kann eine oder mehrere Anwendungen enthalten.
  - Jedes Cluster kann gelöscht werden. Der Link zu Anwendungen wird ebenfalls gelöscht. Die Anwendungen werden nicht gelöscht.
- ✓ Anwendungen (genehmigte Anwendungen im Google Play Store)
  - Anwendungen, die via IKARUS mobile.management-Server-Anwendungen verfügbar gemacht werden
  - Anwendungen, die via IKARUS mobile.management-Server-Anwendungskonfiguration verfügbar gemacht werden

^Home



IKARUS mobile.management - Ansicht oben Play-Store-Layout



Gerät - Play Store (Arbeitsprofil)

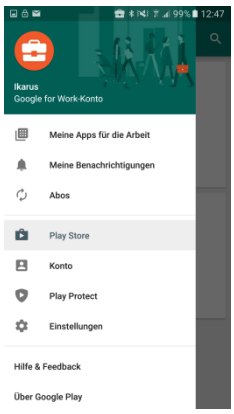
Abbildung 9: Darstellung IKARUS mobile.management-Server und Geräte

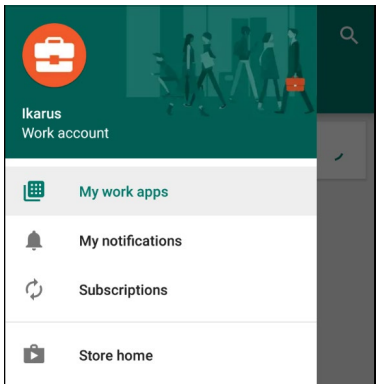
Der Benutzer kann zu jedem Zeitpunkt zum Play Store (Arbeitsprofil) navigieren und auf „My work apps“ *(Meine Arbeits-Apps)* zugreifen, wodurch alle Apps angezeigt werden, die vom Google-Play-Store-Administrator zum Play-Store-Account
hinzugefügt wurden. Der Benutzer kann beliebige genehmigte Apps auswählen und sie direkt auf seinem Gerät installieren.

9.2. Arbeitsprofil – Geräteanzeige

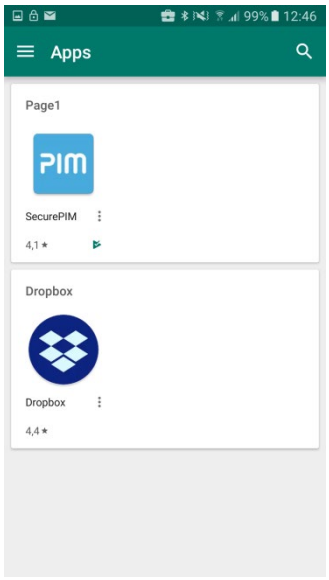
Wenn das Arbeitsprofil installiert ist und der verwaltete Google-Play-Account aktiviert wurde, hat der Benutzer die Möglichkeit, durch Auswahl von „Store Home“ oder „My work apps“ zum Managed Play Store zu navigieren.

Auf dem Benutzergerät: navigieren und Play Store (Arbeitsprofil) öffnen.

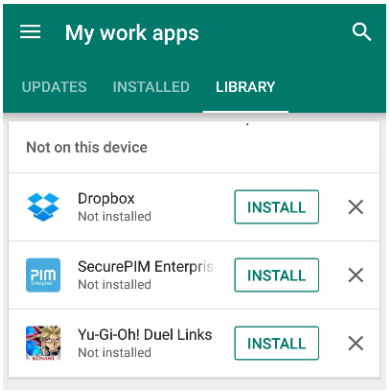




^Home



Store Home

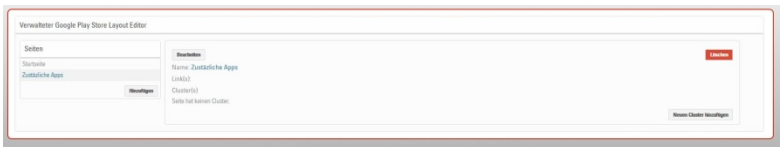


My work apps

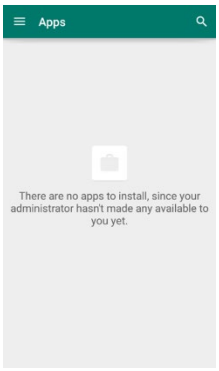
Der Layout-Editor für den Managed Google Play Store des IKARUS mobile.management-Servers ermöglicht es dem Administrator, die verfügbaren Arbeitsprofil-Anwendungen auf dem Benutzergerät in organisierter und benutzerdefinierter Weise zu präsentieren. Er kann nur die Darstellung des „Store Home“ auf der Geräteanzeige beeinflussen.

9.2.1. (Individueller) Layout-Editor für Google Store – Schritt für Schritt

Zum Layout des Managed Google Play Store können zu jedem Zeitpunkt Seiten hinzugefügt werden. Seiten können zusammen mit ihrem Inhalt (Links zu Google Play Store Apps) zudem zu jedem Zeitpunkt entfernt werden.



Layout-Editor-Ansicht



Geräteansicht

9.2.2. Seite 1 (Standardbezeichnung) in Homepage umbenennen

Navigieren Sie zu **Managed Google Work Store layout editor > Pages > Page 1 > Edit** *(Layout-Editor für Managed Google Work Store > Seiten > Seite 1 > Bearbeiten).*

^Home

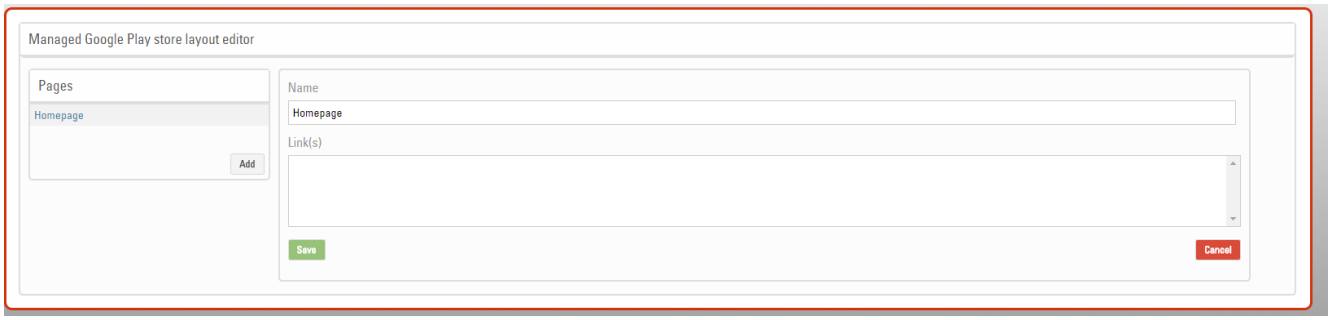


Abbildung 10: Layout-Editor für verwalteten Google Work Store - Seite 1 bearbeiten

Geben Sie einen benutzerfreundlichen Namen ein – in diesem Beispiel wird Homepage verwendet, doch es kann auch der Name Ihrer Organisation verwendet werden. Dann wählen Sie „Save“ *(Speichern)*.

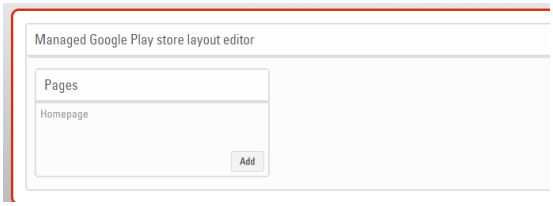


Abbildung 11: Layout-Editor für Managed Google Work Store - Seite 1 umbenennen

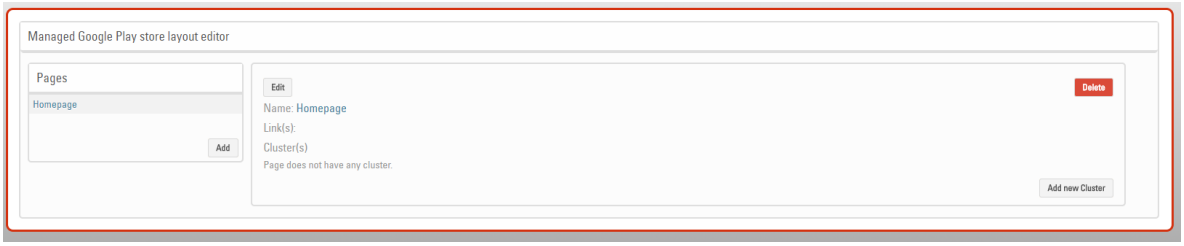
Die Standardseite wurde erfolgreich in „Homepage“ umbenannt.

9.2.3. Beispiel 1

In diesem Beispiel beschreiben wir folgende Aktionen:

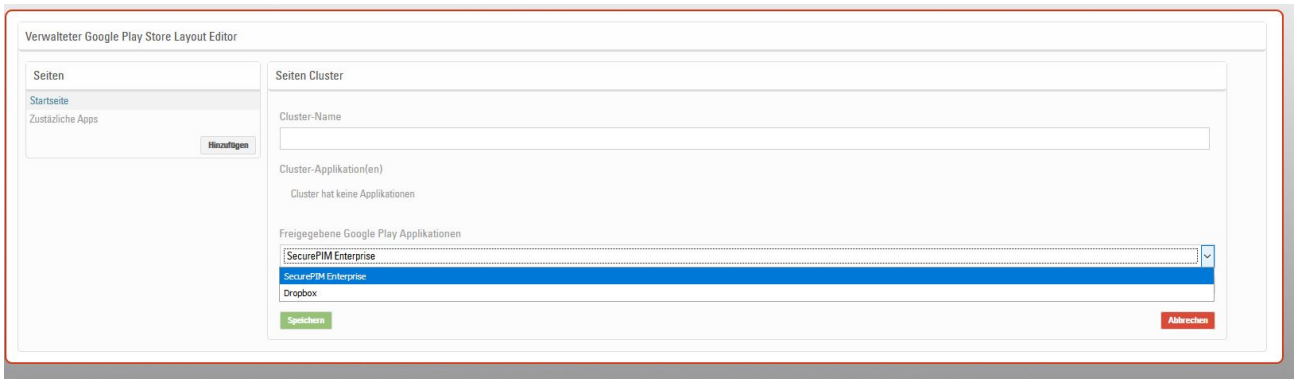
- Umbenennung der Standardseitenbezeichnung „Seite 1” in “Homepage”
- Ein benanntes Cluster zur Seite hinzufügen – „Homepage“
- Hinzufügen einer Anwendung auf der Seite – „Homepage“

Navigieren Sie zu **Managed Google Work Store layout editor > Pages > Page 1 > Edit > Add new cluster** (Layout-Editor für Managed Google Work Store > Seiten > Seite 1 > Bearbeiten > Neues Cluster hinzufügen).

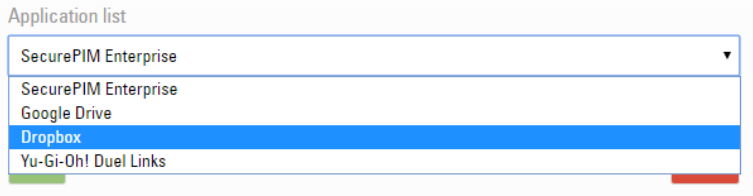


Geben Sie einen benutzerfreundlichen Namen in das Clusternamensfeld ein - in diesem Beispiel „StorageSolutions“.

^Home



Dann wählen Sie die Dropdown-Anwendungsliste aus.



Es erscheint eine Liste mit Anwendungen, die auf dem Google Play Store genehmigt wurden, und allen Android-Anwendungen, die vom Play Store auf den IKARUS mobile.management-Server geladen (und genehmigt) wurden.

Wählen Sie eine Anwendung, in diesem Fall „Dropbox“, und wählen Sie „Add“ *(Hinzufügen).*

Das Anwendungssymbol erscheint auf dem Anwendungsfeld des Clusters - dann wählen Sie „Save“ *(Speichern)*, um den Anwendungslink zum StorageSolutions-Cluster zu speichern.

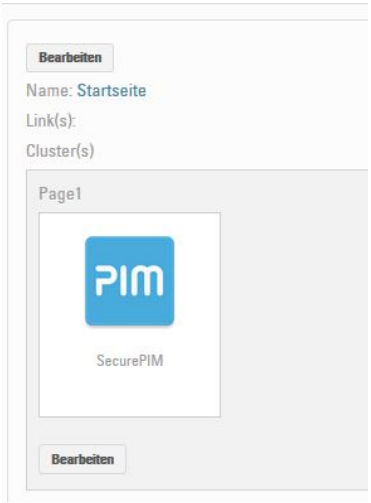
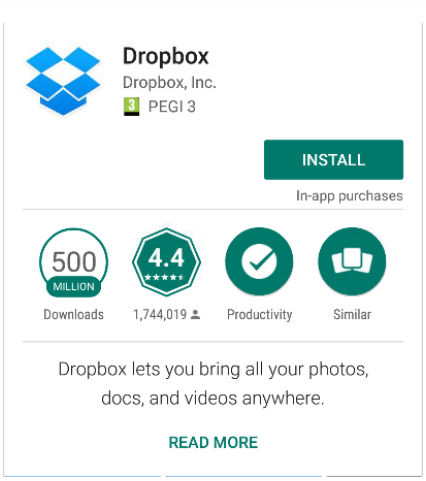


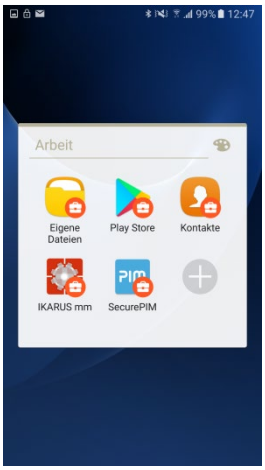
Abbildung 12: Layout-Editor für verwalteten Google Work Store - App hinzufügen

Wenn der Kunde das Dropbox-Symbol auswählt, wird er eingeladen, die Anwendung auf seinem Gerät zu installieren.

^Home



Geräteansicht – Installieren?



Geräteansicht – installiert

Die Anwendung wurde in das Arbeitsprofil des Geräts installiert und wird entfernt, wenn das Arbeitsprofil manuell durch den Benutzer gelöscht wird (Accounts - Arbeit löschen) oder eine Geräterücksetzung vom IKARUS mobile.management-Administrator auf dem Gerät (Arbeitsprofil) ausgelöst wurde.

Alle Apps, die über Google Play for Work installiert sind, sind ohne Einsatz eines lokalen oder Google-Benutzer-Accounts installiert und der Benutzer wird nicht um App-Genehmigungen gebeten, da dies vom Administrator beim Zulassen der App im Voraus akzeptiert wurde.

9.2.4. Beispiel 2

In diesem Beispiel fügen wir eine Seite, einen Link und eine Anwendung hinzu.

Für Beispiel 2 nehmen Sie folgende Aktionen vor (möglichst unter Verwendung Ihrer eigenen genehmigten Anwendungen):

Navigieren Sie zu **Managed Google Work Store layout editor > Pages > Add** *(Layout-Editor für Managed Google Work Store > Seiten > Hinzufügen).*

Add – Name – PIMsolutions, Link Homepage, Save *(Hinzufügen – Name – PIM-Lösungen, Link Homepage, Speichern)*

Homepage > Edit – Highlight Link(s) – PIM Solutions – Save *(Homepage > Bearbeiten – Link(s) markieren – PIM-Lösungen – Speichern)*

Pages > PIMsolutions – Add new cluster *(Seiten > PIM-Lösungen > Neues Cluster hinzufügen)*

Geben Sie einen benutzerfreundlichen Clusternamen ein.

Wählen Sie im Dropdown-Anwendungsverzeichnis „Secure PIM Enterprise – Add“ *(Sicheres PIM-Enterprise – Hinzufügen).*

Die Google-Play-Store-Benutzeroberfläche für das Arbeitsprofils des Benutzers wird typischerweise aktualisiert, wenn der IKARUS mobile.management-Client mit dem IKARUS mobile.management-Server verbunden wird.

^Home

Es ist zu beachten, dass ein Administrator das Layout des Managed Google Play Store verwenden kann:

Seiten

- ✓ Seiten hinzufügen – Diese Seiten können zu jedem Zeitpunkt umbenannt werden.
- ✓ Seiten löschen – Löschen irgendeiner Seite (außer der Standardseite Page 1). Alle Cluster- und Anwendungslink-Daten werden gelöscht. Die Anwendungen werden nicht gelöscht.
- ✓ Seitentitel umbenennen – Nach dem Umbenennen der Seite bleiben die Apps in der bearbeiteten Seite vorhanden.
- ✓ Nur Seiten können Links zu anderen Seiten enthalten.

Cluster

- ✓ Die Seiten können einen oder mehrere Cluster enthalten.
- ✓ Jedes Cluster kann eine oder mehrere Anwendungen enthalten.
- ✓ Jedes Cluster kann gelöscht werden. Der Link zu den Anwendungen wird ebenfalls gelöscht. Die Anwendungen werden nicht gelöscht.

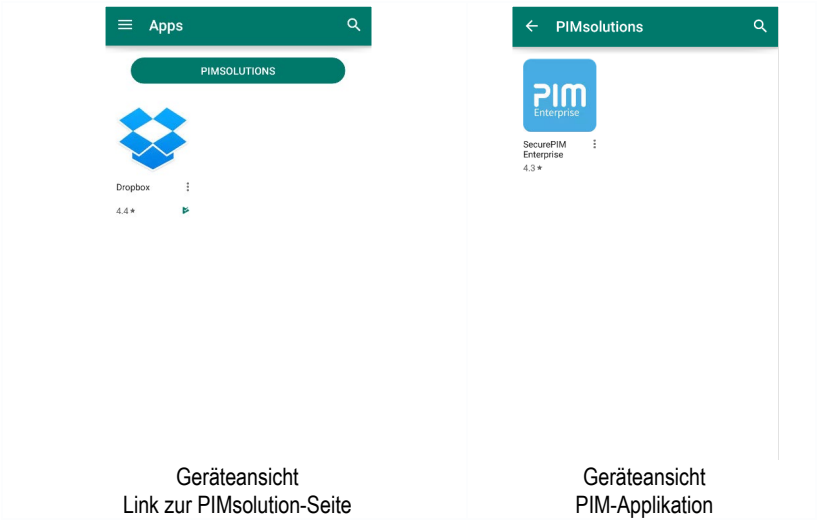
Links (zu anderen Seiten)

- ✓ Links zu den erstellten Seiten hinzufügen (außer auf die eigene Seite)
- ✓ Links zu anderen erstellten Seiten löschen

Es gibt keine (bekannte) Beschränkung für die Anzahl an Seiten, Clustern und Links, die mit dem Managed Google Play Store-Layout-Editor erstellt werden können. Diese Funktion wurde in den IKARUS mobile.management-Server integriert, so dass Benutzer vom Unternehmen genehmigte Anwendungen problemlos finden (und installieren) können. Daher wird ein logischer Ansatz für das Design des vom Unternehmen genehmigten Anwendungslayouts empfohlen:

Daraus ergibt sich Beispiel 2, wie es auf dem Benutzergerät angezeigt wird.

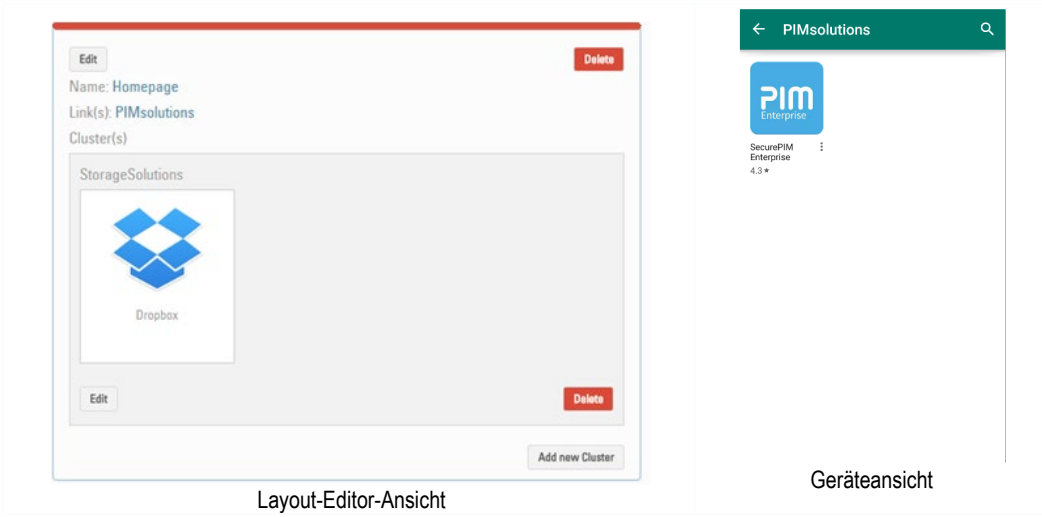
^Home



Geräteansicht
Link zur PIMsolution-Seite

Geräteansicht
PIM-Applikation

Beispiel 2 – Ergebnis des Hinzufügens von Link, Clusterbezeichnung und Anwendung



Layout-Editor-Ansicht

Geräteansicht

Die Anwendung ist nun zum Installieren auf dem Gerät durch den Benutzer verfügbar.

Registerkarte	Beschreibung
Hinzufügen	Neue Seite hinzufügen
Löschen	Löscht die Seite (außer Seite 1 – Homepage)
Name	Wählen Sie den Seitennamen zum Umbenennen des Seitennamens, um Links (zu anderen Seiten) hinzuzufügen oder zu entfernen
Neues Cluster hinzufügen	Fügt ein weiteres Cluster hinzu, das benannt werden kann und zu dem Links zu Anwendungen hinzugefügt werden können

Alle Links zu Anwendungen werden von Google abgerufen.

^Home

10. SecurePIM

SecurePIM ist eine App, die Ihnen sicheren Zugriff auf Ihre E-Mails, Kalender, Dokumente, Kontakte und Aufgaben auf Server-Konten ermöglicht. Außerdem bietet SecurePIM einen sicheren Browser und eine sichere Kamera.

Ihre privaten (Android) Daten bleiben dabei getrennt von Ihren geschäftlichen (SecurePIM) Daten. Die Daten in SecurePIM werden mit neuesten kryptografischen Verfahren in einem Secure Container auf Ihrem Gerät verschlüsselt und E-Mails können signiert und Ende-zu-Ende verschlüsselt ausgetauscht werden.

Ihr SecurePIM Passwort, PIN oder Fingerabdruck schützt diese Daten vor fremden Zugriffen.

Wichtig: Nach der Aktivierung können Sie ausschließlich via SecurePIM mit dem Exchange Server kommunizieren und auf Ihre E-Mails, Kontakte und Kalender zugreifen. Andere Programme können diese Daten nicht mehr abrufen.

11. SecurePIM Installation

Voraussetzungen

Um eine Trennung zwischen privaten und geschäftlichen Daten zu ermöglichen, werden verschiedene Komponenten benötigt. Eine Verwendung bzw. Unterstützung der genannten Komponenten kann von mehreren Faktoren abhängig sein. Die Mindestvoraussetzung für den Einsatz der vorgestellten Lösung sind:

- ✓ 7P EMM System in der Version 5.32.02 oder höher
- ✓ Google Account
- ✓ Android-Endgeräte der Version 6.0 oder höher
- ✓ Android Endgeräte müssen Android for Enterprise / Arbeitsprofil unterstützen
- ✓ Apple iOS 10 oder höher
- ✓ Mailserver: Exchange ActiveSync oder Lotus Notes
- ✓ Optional: Apple DEP und Apple VPP für eine vereinfachte iOS Verwaltung

SecurePIM aktivieren

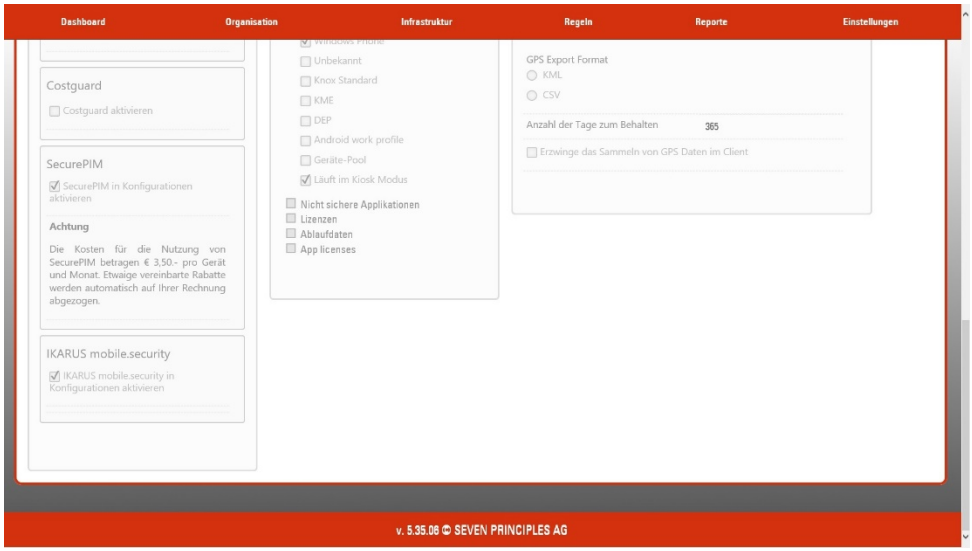
- ✓ Global > Einstellungen/System.
- ✓ Allgemeine Optionen > Bearbeiten Konfigurationen
- ✓ SecurePIM aktivieren

^Home

Achtung!

Die Kosten für die Nutzung von SecurePIM betragen € 3,50 pro Gerät und Monat.

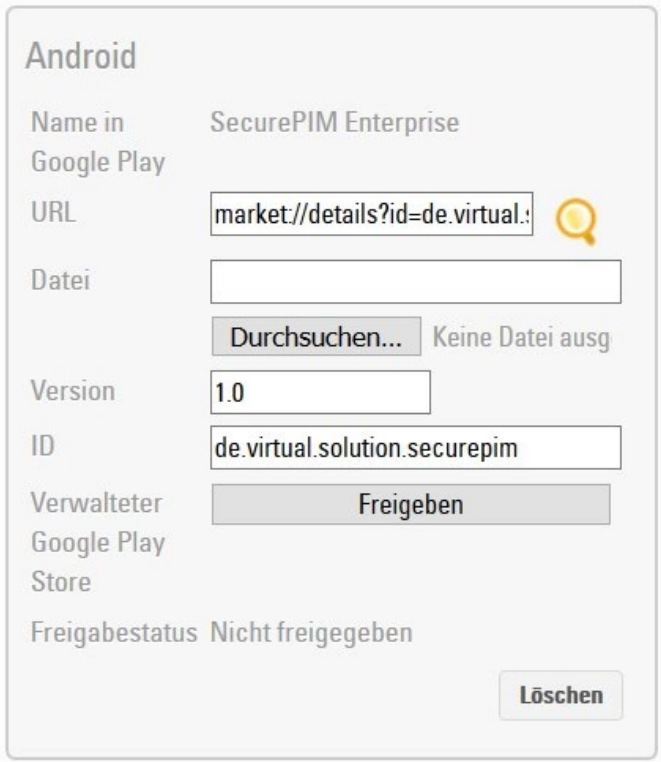
Etwaige vereinbarte Rabatte werden automatisch auf Ihrer Rechnung abgezogen.



Installation via App Store / Play Store

Über Infrastruktur > Applikationen nach SecurePIM suchen.
Für Android klicken Sie bitte auf die angezeigte Schalfläche „Freigeben“ und bestätigen Sie sämtliche Abfragen.

Freigabe deaktiviert	Freigabe aktiviert



^Home

SecurePIM Konfiguration

Default Infrastruktur > Konfigurationen >neue Konfiguration mit dem Konfigurationstyp: SecurePIM

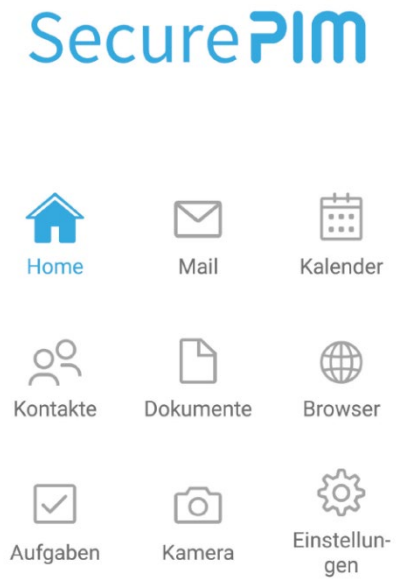
Folgende Parameter sollten eingegeben werden

- ✓ Support-E-Mail
- ✓ Activesync Server
- ✓ E-Mail-Adresse (z.B. in Form eines Platzhalters bzw. Custom Parameters)
- ✓ Benutzername (z.B. in Form eines Platzhalters bzw. Custom Parameters)

Folgende Parametrierung wird außerdem empfohlen:

- ✓ Kontakte: Export zu Caller IDs (CallKit) „Ja“ (zur Auflösung von Rufnummer bei iOS)
- ✓ Kontakte: Export an lokales Verzeichnis „Ja“ (Export von Kontakten in den Arbeitsbereich bei Android)
- ✓ Ort in Erinnerung anzeigen „Ja"
- ✓ Betreff in Erinnerung anzeigen "Ja"

Nun können Sie SecurePIM auf Ihrem Smartphone starten:



^Home