IKARUS mobile.management

Aktivierung der IKARUS mobile.security

Release date: 16.11.2022

Version: 1.1

Die IKARUS mobile.security Applikation ist eine Antiviren und Anti-Malware Anwendung für Endgeräte mit dem Android Betriebssystem.

Dieses Dokument beschreibt den Rollout und die Aktivierung der IKARUS mobile.security (IMS) Applikation via IKARUS mobile.management (IMM)

Zur optimalen Nutzung dieses Dokuments sollten die MDM-Grundlagen, sowie die Menüführung des MDM-Systems bekannt sein.

Vorbereitung

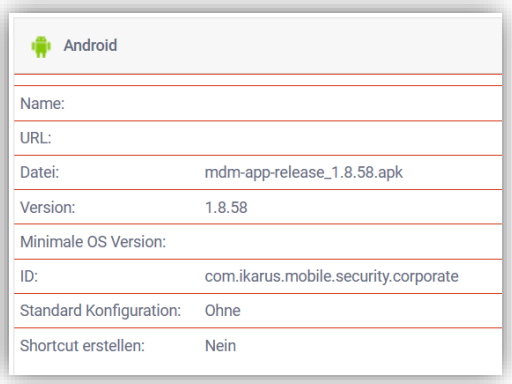
Folgende Vorbereitungen müssen getroffen werden, bevor die IMS-Applikation ausgerollt werden kann.

1. Applikation

1. Legen Sie in Ihrem IMM-System eine neue Applikation für Android an.
2. Laden Sie dort die neuste Version der IMS-Applikation hoch und warten Sie bis die Versionsnummer und die App-ID angezeigt werden.
3. Speichern Sie das Applikationspaket.

Die aktuelle Versionsnummer lautet: 1.8.58

Die neuste Version der IMS-App finden Sie hier: https://mdm.ikarus.at/client/



2. Konfiguration

1. Erstellen Sie eine Konfiguration mit dem Typ „Antivirus“.
2. Legen Sie die Parameter für die Konfiguration fest. – Details finden Sie **hier**.
3. Speichern Sie die Konfiguration

© IKARUS Security Software GmbH

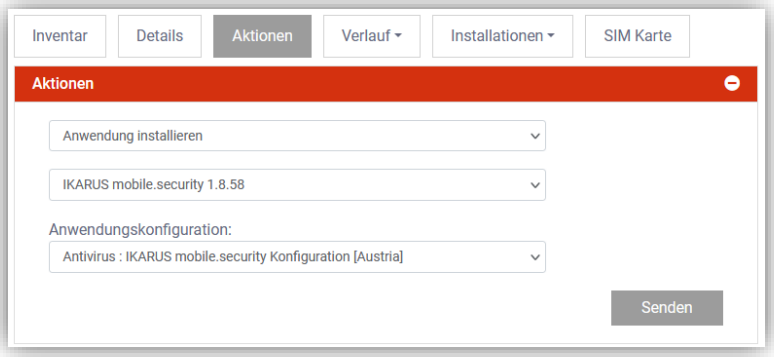
Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Rollout

Um die IMS-Applikation auszurollen, gehen Sie bitte wie folgt vor:

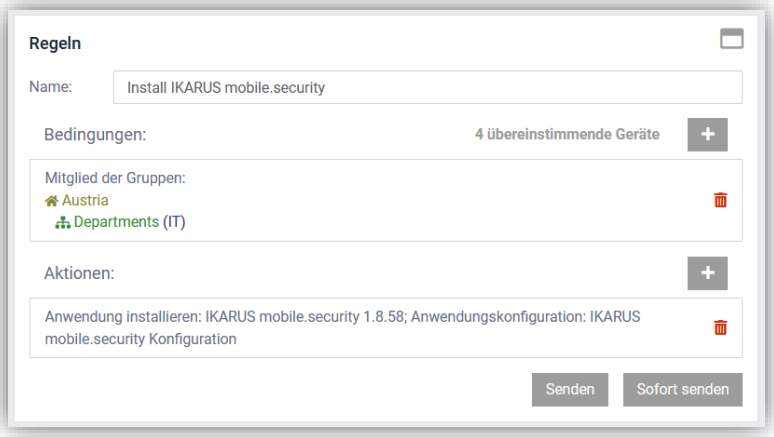
1. Einzelgerät – Aktionen

1. Navigieren Sie zum gewünschten Endgerät unter Organisation > Benutzer und Geräte > Gerät
2. Öffnen Sie das Aktionsmenü des Geräts
3. Wählen Sie aus dem Dropdown-Menü die Aktion **Anwendung installieren** aus
4. Wählen Sie das IMS-Applikationspaket aus
5. Wählen Sie unter Anwendungskonfiguration die zuvor erstellte Konfiguration für die IMS-Applikation aus
6. Drücken Sie auf die Schaltfläche senden



2. Mehrere Endgeräte – Regel

1. Navigieren Sie zum Menü Regeln > Regeln
2. Erstellen Sie eine neue Regel
3. Definieren Sie eine Bedingung, welche die gewünschten Endgeräte für den Rollout erfasst
4. Wählen Sie unter Aktionen „Anwendung installieren“ mit dem IMS-Applikationspaket aus
5. Wählen Sie unter Anwendungskonfiguration die zuvor erstellte Konfiguration für die IMS-Applikation aus.
6. Speichern Sie die Regel
7. Drücken Sie auf die Schaltfläche **senden** um die Aktionen zuzuweisen oder auf **sofort senden** um auch eine Verbindungserzwingung mitzuschicken.



© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Wichtige Hinweise

Lizenzierung

Die Lizenzierung der IKARUS mobile.security Applikation erfolgt über eine Kombination der Komponenten IMS Client und gültiger Konfigurationsdatei. Sind beide Komponenten auf dem Gerät vorhanden und ist das Gerät über das IMM verwaltet, so wird über den Lizenzserver eine Lizenz für das Gerät ausgestellt. Eine Lizenzdatei ist nicht länger erforderlich.

Funktionsumfang

Der Funktionsumfang der IMS-Applikation ist abhängig von mehreren gerätespezifischen Faktoren. Abhängig vom eingesetzten Endgerät und der Betriebssystemversion kann es sein, dass spezielle Features nicht verfügbar sind. Für einige Funktionen kann es erforderlich sein, dass der Gerätenutzer entsprechende Berechtigungen für die Applikation am Gerät manuell vergeben muss.

Installation und Aktivierung

Installation und Aktivierung können abhängig von der MDM-Aktivierungsmethode, vom eingesetzten Endgerät und der Betriebssystemversion variieren. Wird z.B. von einer dieser Komponenten keine silent Installation unterstützt, so kann es erforderlich sein, dass der Gerätenutzer diese Installation manuell bestätigen und spezielle Berechtigungen erteilen muss.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Appendix

Parameter	Erklärung	Empfohlener Wert
Automatische Scans	Legt fest, ob automatische Scans des Geräts durchgeführt werden.	Ja
Intervall zwischen Scans	Legt fest, wie häufig der automatische Scan erfolgt.	Täglich oder zweimal täglich
Voller Scan	Legt fest, ob ein vollständiger Scan des Geräts vorgenommen werden soll oder nur ein Quickscan.	Ja
Automatische Updates	Legt fest, ob die Updates der Datenbank automatischen durchgeführt werden	Ja
Intervall zwischen Updates	Legt fest, wie häufig ein automatisches Update der Datenbank durchgeführt werden soll	Täglich oder zweimal täglich
Automatische Scans von Anwendungen	Legt fest, ob Applikationen gescannt werden sollen	Ja
Automatische Scans des externen Speichers	Legt fest, ob der externe Speicher gescannt werden Ja	Ja
Updates nur über WLAN	Legt fest, über die Datenbank-Updates nur über WLAN erfolgen sollen	Nein
SigQA	Aktiviert eine zusätzliche Reporting Funktion, welche neue aber unbekannte Signaturen an IKARUS übermittelt	Ja
URL Filter	Legt fest, ob der Web-Filter aktiviert werden soll. Diese Funktion ist nur für spezielle native Browser unterstützt und daher nur eingeschränkt verfügbar.	Abhängig vom Use Case.
Eigene URL Blacklist	Nur sichtbar, wenn URL Filter aktiv. Legt eine Liste nicht erlaubter Webseiten fest	Abhängig vom Use Case.
Eigene URL Whitelist	Nur sichtbar, wenn URL Filter aktiv. Legt eine Liste der erlaubten Webseiten fest.	Abhängig vom Use Case.
Web Filter Buttons aktivieren	Legt fest, ob bei aktiviertem Web-Filter beim Aufruf nicht erlaubter Seiten eine überspringbare Warnung angezeigt wird oder die Seite komplett gesperrt wird.	Abhängig vom Use Case.
Infektionen auf dem Gerät anzeigen	Legt fest, ob der User über Virenfunde am Gerät informiert werden soll oder nicht.	Ja
Security Advisor aktivieren	Legt fest, ob der Security Advisor aktiviert werden soll.	Abhängig vom Use Case.

© IKARUS Security Software GmbH

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com