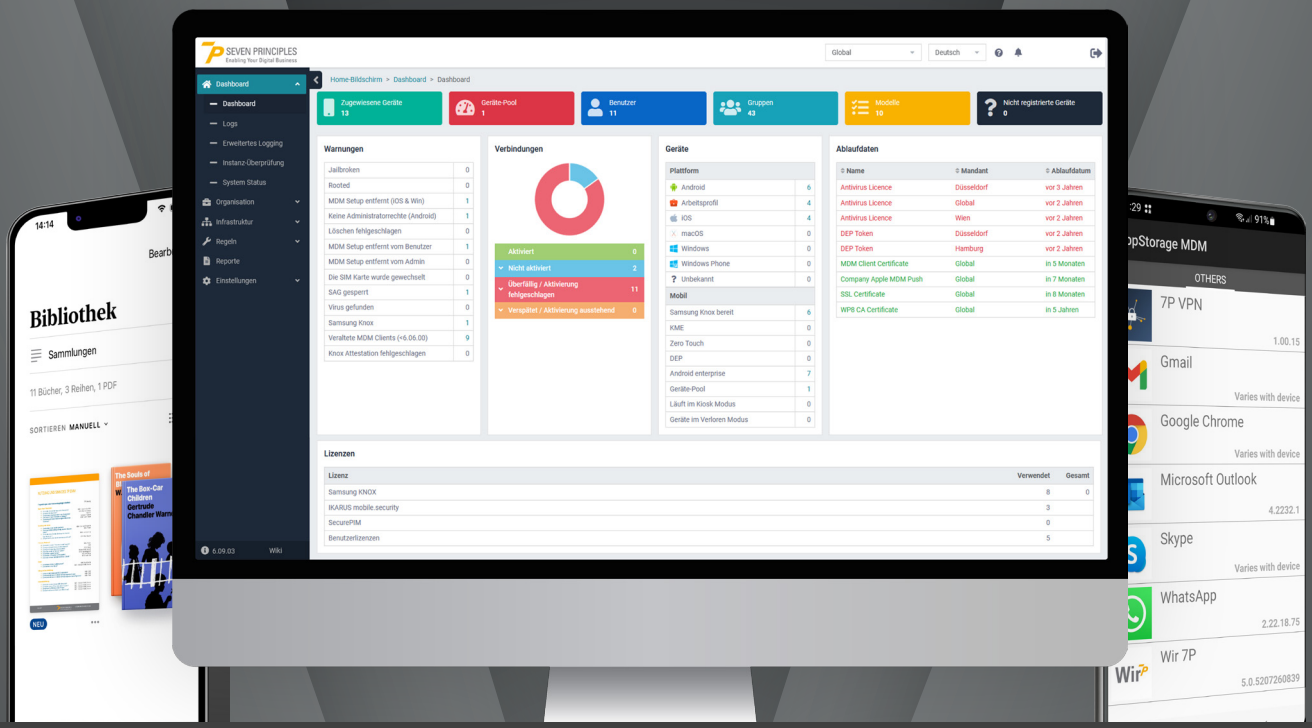
Seven Principles Solutions & Consulting GmbH

7P Enterprise Mobility Management

Die europäische Lösung zur
Sicherung Ihrer Unternehmensgeräte



Featureliste

Inhaltsverzeichnis

Dashboard, UI & Reporting **03**

User & Device Enrollment **03**

Mobile Device Management **04-05**

Mobile Application Management **05-06**

Security & Compliance **07**

AddOns & Interfaces **08**

Dashboard, UI & Reporting

Feature	Beschreibung	iOS	Android
Intuitive und übersichtliche Oberfläche	Das aufgeräumte, übersichtliche Dashboard bietet einen schnellen Überblick über die Informationen, die jede:r Administrator:in ganz individuell sehen möchte, und die einfach zu bedienende Oberfläche reduziert die Bedienzeiten auf ein absolutes Minimum.	✓	✓
Mehrsprachige Bedienoberfläche	Die Bedienoberfläche für Administrator:innen steht Ihnen in deutscher Sprache und 9 weiteren Sprachen zur Verfügung.	✓	✓
Multi-Tenant-Unterstützung	100%ige Mandantenfähigkeit ermöglicht die hierarchische Verwaltung komplexer, organisatorischer oder geografischer Strukturen, unabhängig davon, wo sich die Geräte befinden oder zu welchem Betreibernetz ein Gerät gehört. Ein Super-Admin hat Zugriff auf alle Hierarchien, während ein Mandanten-Admin nur Zugriff auf die Geräte und Benutzer der ihm zugeordneten Organisation hat.	✓	✓
Reporting	Detaillierte Berichte über Geräte, Benutzer:innen und Anwendungen erstellen, exportieren und automatisiert versenden.	✓	✓

User & Device Enrollment

Feature	Beschreibung	iOS	Android
Automatisiert Geräte ausrollen	Leistungsstarke MDM-Engine für die Massenbereitstellung von Geräten, die alle wichtigen Enrollment-Programme unterstützt. Dazu gehören Apple ADE (Automated Device Enrollment, ehemals Apple DEP), Samsung Knox Mobile Enrollment und Android Zero-Touch	✓	✓
Individuelle Geräteregistrierung	Durch einfache Registrierung über QR-Code werden alle MDM-Profile automatisch auf dem Gerät installiert. Das Gerät kann dann vollständig konfiguriert an den:die Nutzer:in übergeben werden.	✓	✓
Unternehmensintegration	Die Integration mit Microsoft Entra ID (ehemals Azure Active Directory) oder eDir über LDAP ermöglicht den automatischen Import von Benutzer:innen und Gruppen.	✓	✓
CSV-Import	User und Gruppen von Benutzer:innen können bequem über einen CSV Import angelegt werden.	✓	✓
Self Service Portal	Das Self Service Portal ermöglicht es Endbenutzer:innen, Geräte selbst zu registrieren.	✓	✓

Mobile Device Management

Feature	Beschreibung	iOS	Android
Sicheres Gerätemanagement	7P-EMM unterstützt sicher Bring Your Own Device (BYOD), Corporate-Owned Personally Enabled (COPE) und andere Mobile Device Management Strategien.	✓	✓
Management von Richtlinien	Flexibles Konfigurieren, Verwalten und Ausrollen von Unternehmensrichtlinien pro Benutzer:in, Benutzergruppe, Mandant:in oder Plattform. Erstellung von Richtlinien für mobile Strategien wie BYOD, firmeneigene Geräte oder Kiosk-Geräte.	✓	✓
Verwalteter Google Play Store	Ein verwalteter Google Play Store erleichtert die Administration verbessert die Sicherheit und Kontrolle über die Anwendungen. Mit einem verwalteten Google Play Store können Sie Ihre eigenen Anwendungen (Apps) in einem privaten App-Store hosten, der nur für ihre Mitarbeiter:innen zugänglich ist. Das bedeutet, dass die Benutzer:innen nur die Anwendungen sehen und herunterladen können, die von Ihrer Organisation genehmigt wurden.		✓
E-Mail Push	Automatisierte Einrichtung der E-Mail-Accounts. Die Einstellungen werden OTA (over-the-air) an Mitarbeitende, Benutzer:innengruppen oder das gesamte Unternehmen verteilt.	✓	✓
WLAN Konfiguration Push	Die Konfiguration der WLAN-Profile kann OTA erfolgen und die Einstellungen können direkt auf das Gerät gepusht werden. Der:die Nutzer:in wird ohne weitere Eingaben direkt und automatisch mit dem WLAN verbunden.	✓	✓
VPN Konfiguration Push	Die VPN-Einstellungen werden automatisch für Einzelnutzer:innen, Gruppen von Nutzer:innen oder das Gesamtunternehmen auf die Geräte ausgerollt – inkl. Apples Per-App VPN. Für beide Betriebssysteme wird eine zusätzliche App benötigt.	✓	✓
Dual-SIM-/eSIM-Support	7P-EMM ermöglicht die Verwaltung von Dual-SIMs, unabhängig davon, ob es sich um physische Karten oder eSIMs handelt.		✓
BYOD (Bring Your Own Device)	Eine umfassende BYOD-Strategie kann mit einem Höchstmaß an Sicherheit und zahlreichen Kontrollmöglichkeiten umgesetzt werden. Unterstützt werden iOS User Enrollment (erfordert iOS 13.1+) und Android Arbeitsprofile.	✓	✓
Geteiltes iPad für Unternehmen und Schulen	In Kombination mit dem Apple Business Manager und Apple School Manger können geteilte iPads konfiguriert und von Benutzer:innen verwendet werden, ohne dass diese eine Apple ID benötigen.	✓	
Betriebssystem-Updates verwalten	Erzwingen oder Verzögern der Installation neuer Betriebssystem-Updates.	✓	✓

Feature	Beschreibung	iOS	Android
Automatisches Durchsetzen der Compliance Richtlinien	Nach möglichen Regelverstößen wie Jailbreak oder der Installation einer nicht erlaubten App kann der Client automatisch blockiert oder die Daten partiell ferngelöscht werden	✓	✓
Corporate Design	Passen Sie Ihre Geräte an das Corporate Design Ihres Unternehmens an, z.B. durch Anpassung des Hintergrunds mit einem eigenen Bild (nur für vollverwaltete Geräte).	✓	✓
GPS Location Tracking	Die Geräte können (unter voller Berücksichtigung der EU-DSGVO) mittels GPS Tracking geortet und der Standort kann direkt auf einer Karte angezeigt werden.	✓	✓

Mobile Application Management

Feature	Beschreibung	iOS	Android
Anwendungs- und Konfigurations-management	Anwendungen im EMM automatisiert konfigurieren und komfortabel an Benutzer:innen oder vordefinierte Gruppen von Benutzer:innen ausrollen.	✓	✓
Eigene und Drittanbieter Apps	Intranet- und Internetanwendungen sowie eigenständig entwickelte oder Drittanbieter-Apps zentral verwalten und Nutzer:innen OTA zur Verfügung stellen. (*.APK- oder *.IPA-Apps)	✓	✓
7P Enterprise-App-Store	Die 7P-App umfasst einen Enterprise-App-Store, den Administra-tor:innen einfach für ihre Anwender:innen bereitstellen können. Die Benutzer:innen sehen nur die obligatorischen und optionalen Apps, die sie benötigen, und können sie direkt aus der App herunterladen.	✓	✓
Strenge Trennung geschäftlicher und privater Daten	Für iOS und Android kann ein nativer Container für Business Apps erstellt werden, der den Datenaustausch mit privaten Apps verhindert.	✓	✓
Blacklist/Whitelist - Apps	Steuern Sie, welche Anwendungen Sie auf den Endgeräten der Mitarbeitenden freigeben und welche Sie verbieten wollen.	✓	✓
Apple Business Manager	7P-EMM unterstützt vollumfänglich den Apple Business Manager. Apps können zentral gekauft, verwaltet und den Mitarbeitenden zur Verfügung gestellt werden, auch in großen Mengen und ohne jegliche Benutzerinteraktion. Die Mitarbeiter:innen benötigen keine eigene Apple ID.	✓	

Feature	Beschreibung	iOS	Android
Application Push/ Managed Apps	Anwendungen als Managed Apps auf die Geräte verteilen. Dabei festlegen, mit welchen Unternehmensdaten diese kommunizieren dürfen. Auf Anwenderseite sind keine Installationsschritte erforderlich.	✓	✓
Automatic App Updates	7P-EMM kann neue App-Updates automatisch auf den Geräten installieren. Dies gilt für Pflicht-Apps auf Android- und iOS-Geräten.	✓	✓
iOS-/iPadOS-Updates	Steuern Sie mit 7P-EMM die iOS-/iPadOS-Updates um z.B. wichtige Sicherheits-Updates zur erzwingen.	✓	
Konfiguration verwalten	Zentrale Konfiguration von Berechtigungen und Konfigurationen für alle App-Nutzer:innen.	✓	✓
Kiosk Mode	7P-EMM kann Android Geräte in einen Kiosk Mode versetzen, d.h. es können nur bestimmte Apps gestartet werden, alle anderen Apps sind nicht zugänglich. Der:die Anwender:in kann diese Apps nicht schließen oder das Gerät für andere Zwecke nutzen. Der Zugriff auf OS-Einstellungen etc. kann verweigert werden.		✓
iOS Einzel-App-Modus	Der Einzel-App-Modus ermöglicht es, das Öffnen einer bestimmten App auf einem verwalteten Gerät zu erzwingen und zu verhindern, dass andere Apps auf dem Gerät verwendet werden. Die App wird nach dem Neustart sofort wieder geöffnet.	✓	

Security & Compliance

Feature	Beschreibung	iOS	Android
Passwort- Richtlinien	Festlegen von Passwortrichtlinien, z.B. Passwortlänge, maximale Passwortgültigkeit oder Erfordernis eines alphanumerischen Passworts.	✓	✓
Remote Wipe	Unternehmensdateien vor unautorisiertem Zugriff schützen dank der Möglichkeit, einen kompletten Remote Wipe durchzuführen.	✓	✓
Unterstützung von Policies	Die Lösung unterstützt iOS- und Android-Policies. Weitere Policy-Einstellungen sind möglich.	✓	✓
Remote Lock	Firmengeräte können aus der Ferne gesperrt werden. Zum Entsperren ist anschließend ein Passwort nötig.	✓	✓
Lost Mode	Der Zugriff auf verlorene oder gestohlene Geräte kann durch Aktivieren des Lost Modes (“Verwalteter Modus Verloren”) verhindert werden. Dieser Modus ermöglicht zusätzliche Sicherheitsfunktionen wie die Lokalisierung des Geräts, das Zurücksetzen des Passworts oder das Löschen der Daten dem Gerät.	✓	
Alarmierung	Spielen Sie über das EMM einen Alarmton an einem oder mehreren Geräten gleichzeitig ab.	✓	✓
Samsung Knox Attestation	Mit der Samsung Knox Attestation können Sie überprüfen, ob ein Samsung Android-Gerät mit Root-Software oder inoffizieller Firmware ausgestattet ist, die die Datenintegrität gefährden kann.		✓
Google Play Integrity	Die Google Play Integrity API löst die Google SafetyNet Attestation ab und bietet erweiterte Funktionen, um Apps auf deren Integrität zu prüfen. So lässt sich beispielsweise ermitteln, ob es sich bei der installierten App um die Originaldatei handelt und ob sie von einem registrierten Benutzer installiert wurde.		✓
Zertifikatsunterstützung für iOS und Android	Zertifikate können über die EMM Konsole ausgerollt und überwacht werden (z.B. Ablaufdatum)	✓	✓
SCEP Support	Unterstützung des Simple Certificate Enrollment Protocol (einfaches Zertifikat-Registrierungs-Protokoll, kurz SCEP) konfigurieren, um Zertifikate bereitzustellen. Auf diese Weise können Geräte Zertifikate über SCEP bei einer Zertifizierungsstelle beziehen.	✓	✓
Root- und Jailbreak-Erkennung	Von Rooting oder Jailbreaking betroffene Geräte werden automatisch erkannt und im Dashboard angezeigt.	✓	✓
Management von WiFi-Profilen	WiFi-Profile können einfach erstellt und Nutzern bzw. Nutzergruppen zugeteilt werden.	✓	✓
Globale HTTP- Proxys	Festlegen von globalen HTTP-Proxy-Einstellungen (nur bei verwalteten Geräten)	✓	

AddOns & Interfaces

Feature	Beschreibung	iOS	Android
IKARUS mobile.security	IKARUS mobile.security schützt Ihr Gerät und Ihre Daten verlässlich und effizient mithilfe täglicher Updates und definierbarer Scan-Intervalle. Der Status der Geräte ist direkt im 7P-EMM Dashboard ablesbar.		✓
SecurePIM	SecurePIM für iOS und Android vereint alle wichtigen Funktionen, wie E-Mail, Messenger, Telefonie, Kalender, Dokumente und vieles mehr, in einer einzigen Anwendung. Die Container-Technologie sorgt dabei für höchste Sicherheitsstandards mit verschlüsselten Daten und echter Ende-zu-Ende-Verschlüsselung.	✓	✓
Check Point Harmony Mobile	Eine der umfassendsten Threat Defense Lösungen, die aufkommende Cyberangriffe der fünften Generation verhindert. Harmony Mobile ist fest im 7P-EMM-System integriert und bietet eine Risikobewertung des Geräts, die 7P-EMM nutzt, um das Gerät unter Quarantäne zu stellen oder eine Reihe von Richtlinien zu aktivieren, bis das Gerät nicht mehr gefährdet ist. Der Status der Geräte ist direkt im 7P-EMM Dashboard ablesbar.	✓	✓
Teamwire Messenger	Der sichere Business Messenger für mobile Zusammenarbeit bietet Chatfunktionen, Videokonferenzen & vieles mehr, 100% DSGVO-konform und mit den Sicherheitsstandards der Polizei.	✓	✓
Apple School Manager	7P-EMM arbeitet eng mit dem Apple School Manager zusammen, um Schulen optimal bei der Verwaltung digitaler Lerngeräte zu unterstützen. Die für den Schulbetrieb angepasste Lösung und der ‚Geteiltes iPad Mode' von Apple sorgen dafür, dass iPads datenschutzkonform und sicher von verschiedenen Schüler:innen genutzt werden können. Lehrer:innen behalten dabei die Kontrolle über jedes iPad, damit alle Lernenden konzentriert arbeiten können – ob im Klassenzimmer oder beim Fernunterricht.	✓	
Microsoft "Bedingter Zugriff"	Gerätekompatibilitätsrichtlinien gewährleisten die sichere Integration in Microsoft-Funktionen und -Dienste wie Microsoft 365 (Erfordert eine gültige Lizenz für die Nutzung des Microsoft Intune®-Dienstes.)	✓	✓

Seven Principles Solutions & Consulting GmbH

Ettore-Bugatti-Straße 6-14
51149 Köln

E-Mail: emm@7p-group.com
Internet: www.7p-emm.com

Nehmen Sie jetzt Kontakt auf