baramundi

Whitepaper

Enterprise Mobility Management

Was leisten Managementlösungen heute?

Empower your IT

INHALT

1 Enterprise Mobility Management (EMM)

Der Gebrauch von mobilen Geräten ist in vielen Unternehmen zum Standard geworden und viele Mitarbeiter wollen von ihren eigenen mobilen Geräten aus auf Unternehmensdaten zugreifen. Für Firmen kann das einige Vorteile bringen, allerdings sollten sich die IT-Verantwortlichen der Risiken bewusst sein. Damit sich Notebooks, Tablets und Smartphones sicher in den Berufsalltag integrieren lassen, ist ein effektiver Schutz samt einer Inventarisierung Grundvoraussetzung.

Smartphones und Tablets sind als tragbare Computer annähernd den gleichen Bedrohungen ausgesetzt wie stationäre PCs. In den letzten Jahren waren mobile Systeme durch Viren sehr unter Beschuss. Experten verzeichneten so viele unterschiedliche Schadsoftware-Arten wie nie zuvor. Dabei zeichnet sich ein neuer Trend ab: Immer häufiger kopiert mobile Malware die Funktionen und Auswirkungen von Schadsoftware auf dem Desktop-PC. Dagegen müssen sich Unternehmen wappnen. Wenn Unternehmen sich erstmals mit einer Mobility-Strategie und in diesem Zusammenhang mit der Einführung einer EMM-Software – als Ergänzung zum Client-Management oder als Standalone-EMM-Suite – befassen, gilt es zunächst einige wichtige Fragen zu klären, um die passende Lösung zu finden.

- Wie einfach können Mobilgeräte in die Management-Lösung aufgenommen werden?
- Können die Geräte inventarisiert werden?
- Können mit der Lösung mobile Geräte konfiguriert werden?
- Welche Sicherheitsfunktionalitäten sollte die EMM-Lösung bieten?
- Unterstützt die EMM-Lösung spezielle Business-Funktionalitäten wie das Apple Volume Purchase Programm?
- Integriert vs. Standalone: Welche Lösung eignet sich für wen?
- Wie ist es um die Bedienbarkeit der Software bestellt?
- Können heterogene Betriebssysteme effizient verwaltet werden?

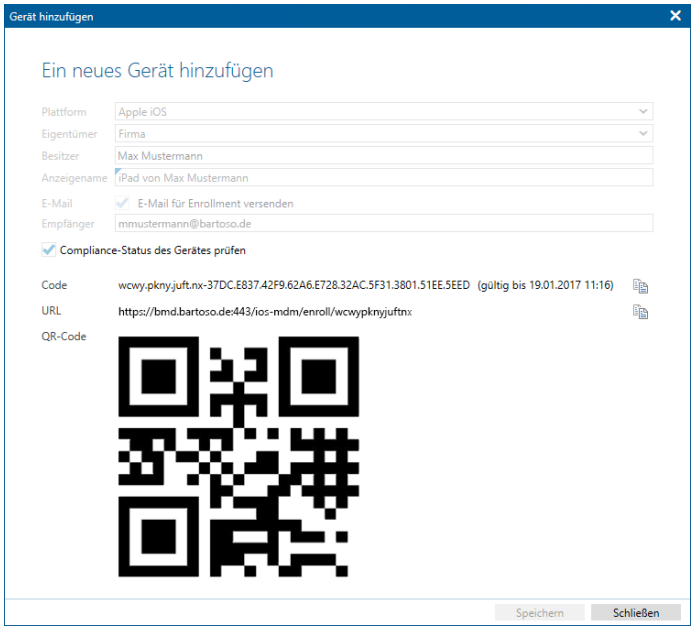
Daraus ergibt sich dann eine Art persönliche Anforderungsliste, welche die Grundlage bildet, um die verschiedenen Anbieter gezielter zu betrachten und eine Vorauswahl passender Lösungen zu treffen. Auf Basis dieser individuellen Shortlist sollten Administratoren dann EMM-Suiten in der Praxis testen und bewerten. Das Ziel bei der Verwaltung von Mobilgeräten ist dasselbe wie bei PC-Clients: Effektiv einen störungsfreien Betrieb sicherstellen, stets den Überblick über den Zustand der Geräte behalten und Sicherheit gewährleisten. Mithilfe einer Enterprise-Mobility-Management-Lösung können Mobilgeräte umfassend verwaltet und abgesichert werden.

2 Automatisiert managen und Sicherheit gewährleisten

2.1 Enrollment

Zur Verwaltung über eine EMM-Lösung müssen die betreffenden Mobilgeräte zunächst in die Lösung aufgenommen und beim Managementserver angemeldet werden. Das Enrollment sollte einfach ablaufen und möglichst auch für einen Nutzer ohne IT-Kenntnisse über eine Netzwerkverbindung möglich sein – speziell, wenn ein Bring-Your-Own-Device-Szenario umgesetzt werden soll.

Ein Beispiel: Der Administrator erzeugt einen QR-Code und schickt ihn per E-Mail an einen Nutzer. Dieser scannt den Code auf seinem Bildschirm mit dem neuen Smartphone, bestätigt die Verwaltung durch die EMM-Suite und das Gerät kann fortan verwaltet werden.



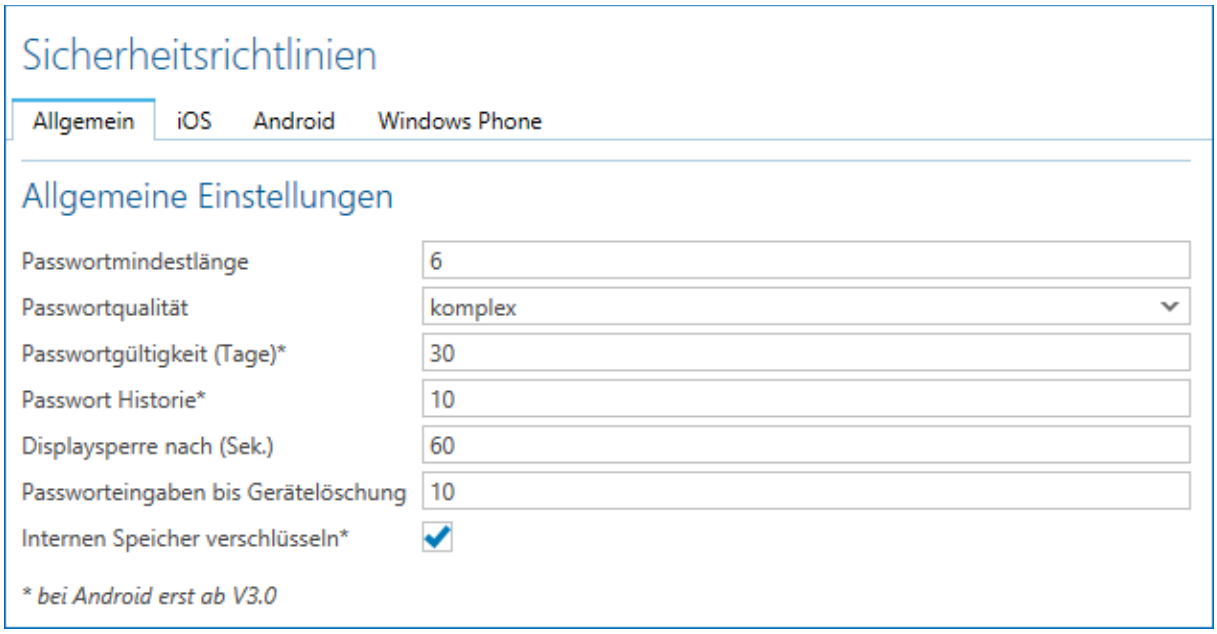
Enrollment mit baramundi Mobile Devices

2.2 Inventarisierung

Welche Geräte befinden sich eigentlich in meinem Netzwerk und was ist auf diesen Geräten installiert? Eine EMM-Lösung sollte grundlegende Antworten auf diese Fragen zu allen populären Betriebssystem-Plattformen bereitstellen können. So können auf iOS-, Android- und Windows-Mobilgeräten mit der Lösung Informationen zur Hardware und Sicherheitseinstellungen sowie den installierten Apps und Zertifikaten gesammelt werden.

2.3 Passwortschutz erzwingen

Um die wertvollen Firmendaten zu sichern, ist zuverlässiger Schutz vor unbefugten Zugriffen durch ein starkes Passwort nötig. Dies kann auf den mobilen Plattformen mit einer EMM-Lösung erzwungen werden. Dabei ist es möglich, die Komplexität des Passwortes vorzugeben, um zu verhindern, dass Nutzer eine ebenso unkomplizierte wie unsichere Kombination (z. B. „1234“) verwenden. Richtlinien für die Geräteverschlüsselung können dort, wo sie nicht ohnehin schon aktiv sind, nachträglich aktiviert werden.



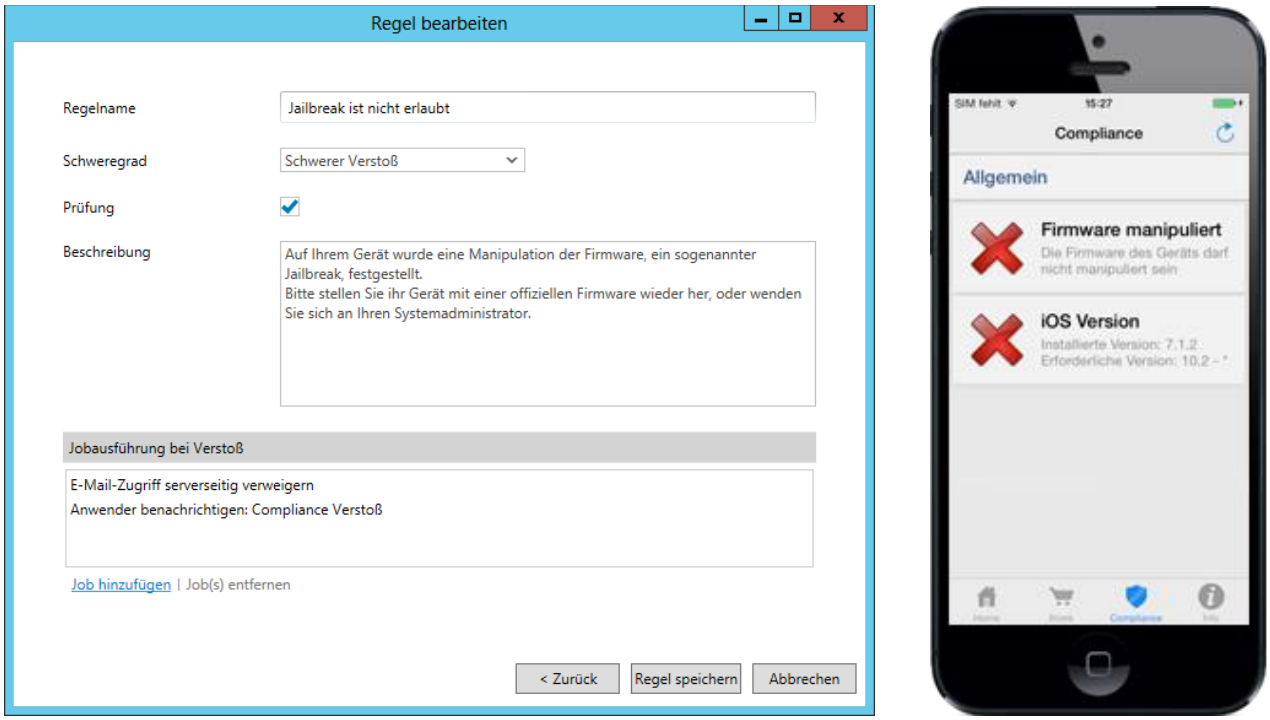
Konfiguration eines Sicherheitsprofils

2.4 Remote sperren und löschen

Ist das Gerät verloren gegangen, lassen sich je nach Plattform die Geräte per Fernsteuerung („remote“) sperren und löschen. Vergisst der Benutzer sein Passwort, kann der Administrator aus der Ferne helfen, das Gerät zu entsperren.

2.5 Jailbreak- und Root-Erkennung

Mit den Begriffen Jailbreak (bei iOS-Geräten) oder Root (unter Android) werden Modifikationen der Firmware eines mobilen Gerätes bezeichnet. Derartige Änderungen erlauben dem Nutzer zum Beispiel die Installation von Anwendungen oder das Freischalten von Funktionen, die vom Hersteller nicht vorgesehen und freigegeben sind. Anleitungen zur Durchführung kursieren im Internet. Durch einen Jailbreak oder ein gerootetes Smartphone sind die Schutzfunktionen des Betriebssystems ausgehebelt. Das Risiko, sich dann Schadsoftware einzufangen, steigt damit stark an. Zudem ist die Verwaltung eines entsperrten Geräts über die EMM-Lösung nur eingeschränkt möglich, weil dessen Schutzfunktionen umgangen werden können. Daher sollten Unternehmen grundsätzlich eine derartige Modifikation des Betriebssystems über entsprechende Compliance-Prüfungen überwachen.

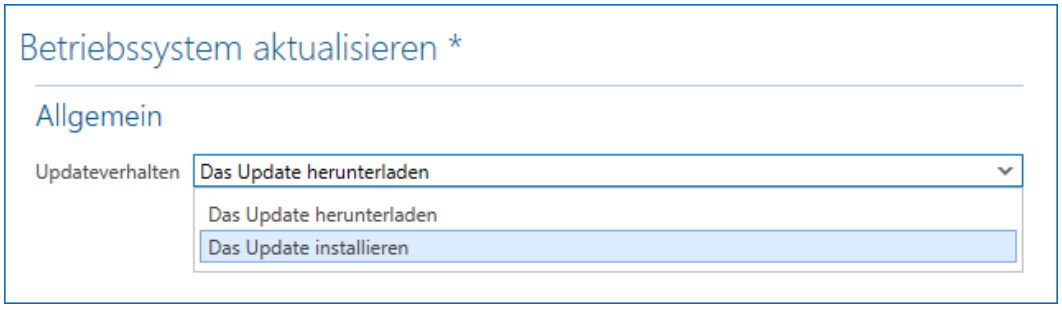


Prüfung auf Jailbreaks

Unter Sicherheitsaspekten gelten derart modifizierte Geräte als äußerst kritisch. Derartige Eingriffe sollten von einer EMM-Lösung erkannt werden. Auch dem Endbenutzer kann über eine verbundene Management-App ein solcher Compliance-Verstoß – oder auch andere – aufgezeigt werden.

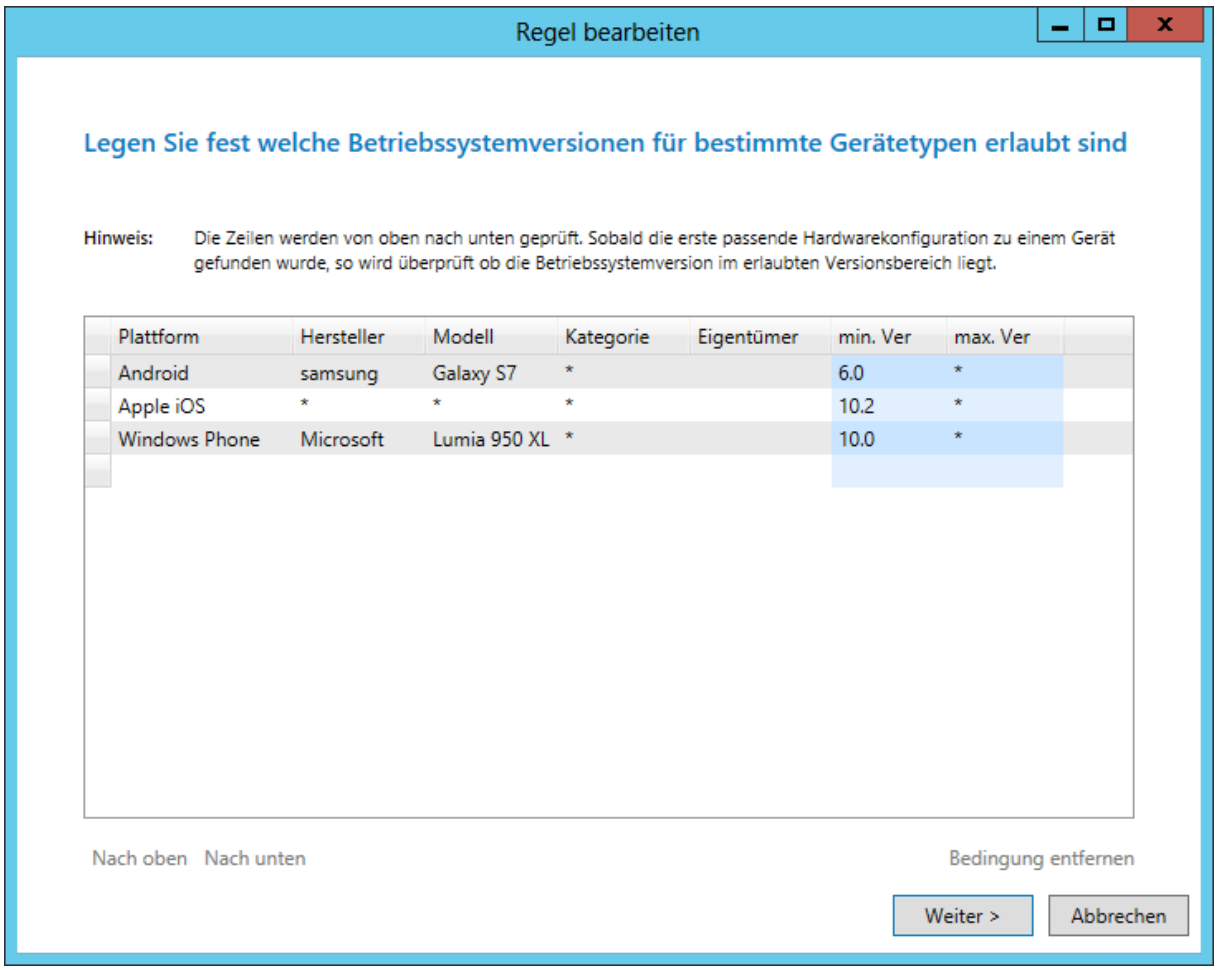
2.6 Aktualisierung der Firmware

Ebenso wichtig wie das Unterbinden von Firmware-Manipulationen ist das zeitnahe Aktualisieren der Firmware, sobald der Hersteller eine neue Version anbietet. Diese bringt in der Regel nicht nur neue Funktionen, sondern beseitigt auch Schwachstellen. Derartige Upgrades können auf modernen Plattformen bereits ferngesteuert werden.



Betriebssystem-Update per Fernsteuerung

Auf allen Plattformen ist eine Überwachung der Firmware-Stände möglich. Per Inventur oder – noch eleganter – per automatisch zu prüfenden Compliance-Regeln kann sich der Administrator jederzeit einen Überblick aus der Ferne verschaffen.

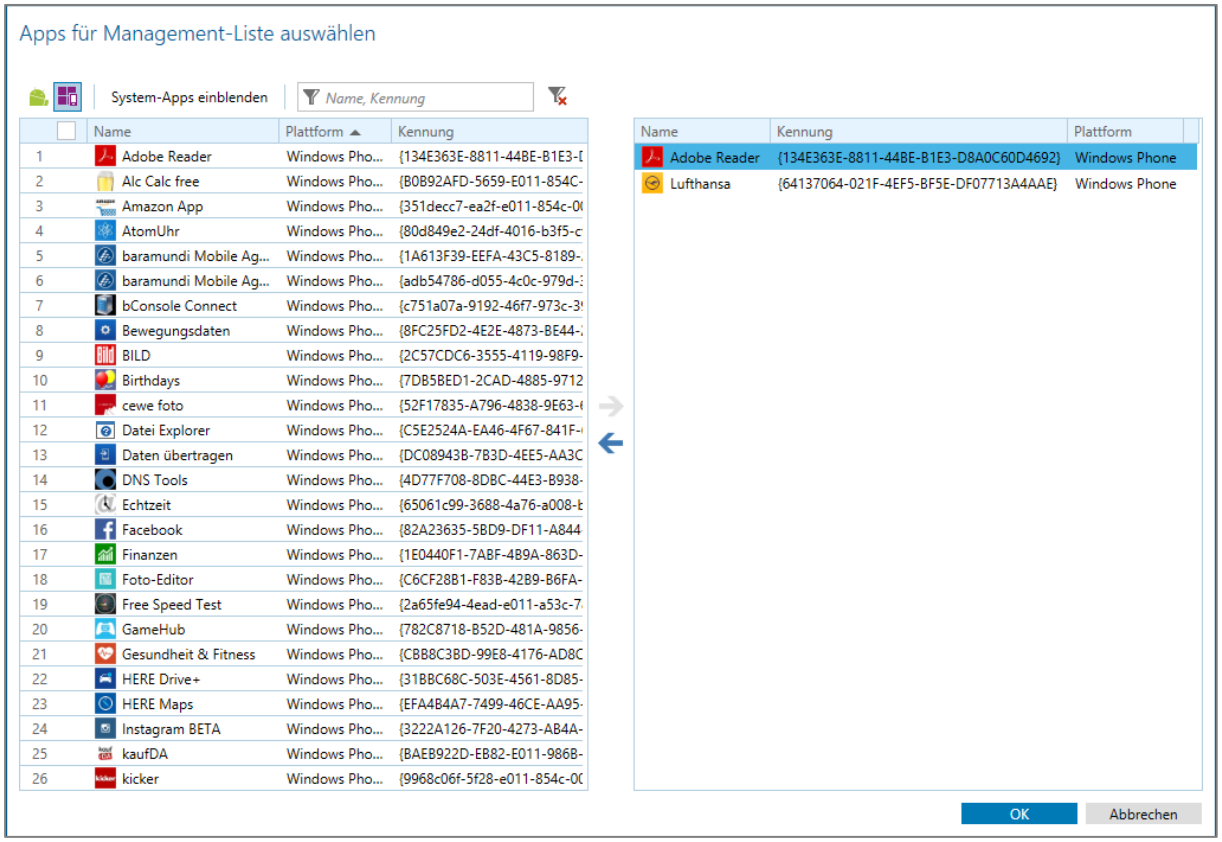


IT-Compliance-Regeln für Betriebssystemversionen

2.7 App-Black- und Whitelisting

Um die Ausführung gefährlicher Apps zu verhindern oder eine Auswahl als vom Unternehmen vertrauenswürdig eingestufter Apps anzubieten, sollte die Lösung App-Black- bzw. Whitelisting unterstützen. Dann kann der Administrator auf kompatiblen Mobilgeräten die Installation bzw. Ausführung ungewünschter Apps unterbinden. Umgekehrt ermöglicht der Whitelisting-Ansatz, explizit erlaubte Apps zu definieren, so dass alle nicht gelisteten Apps an der Installation bzw. Ausführung gehindert werden.

Je nach Präferenz des Administrators kann entweder Whitelisting oder Blacklisting für ein jeweiliges Endgerät genutzt werden. Nach der Entscheidung für den Listentyp, werden die gewünschten Apps der Liste hinzugefügt und dann als Profil auf das Mobilgerät übertragen.



App-Auswahl für Black- oder Whitelisting

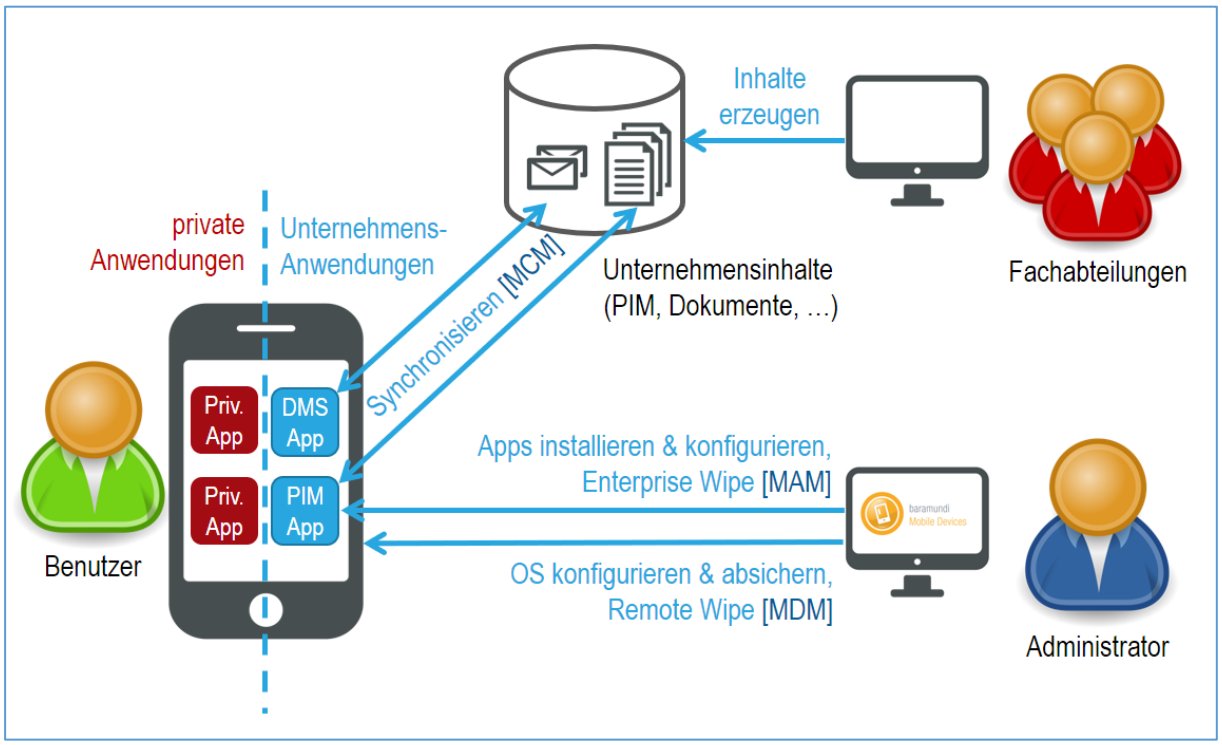
Der Administrator sieht ferner mit Hilfe einer geeigneten EMM-Lösung auf einen Blick, ob eine zuvor installierte App ausgeführt werden kann oder nicht. Mit derartigem App-Listen kann sich das Unternehmen wirkungsvoll gegen Malware-Apps schützen.

2.8 App-Konfiguration

Enterprise Mobility Management umfasst bekanntlich als Überbegriff mehrere Teildisziplinen des Managements mobiler Geräte. Die wesentlichen drei Aspekte hierzu sind Mobile Device Management (MDM), Mobile Application Management (MAM) und Mobile Content Management (MCM), gemeint ist damit das Management des gesamten Geräts, der einzelnen Apps und schließlich der Inhalte. Inwiefern unterstützt die baramundi-Lösung ganzheitliches EMM?

Als aktives Mitglied der AppConfig Community, eine Initiative führender EMM-Hersteller, hat sich baramundi dem Ziel verschrieben, die Verteilung und Konfiguration von Apps unter Nutzung von nativen Mitteln von Betriebssystemherstellern zu vereinfachen. Die Suite bietet vielfältige Funktionalitäten zu MDM und MAM und wird durch geeignete Apps von Drittanbietern aus dem DMS/PIM-Umfeld um MCM-Funktionalitäten ergänzt. Die Verbindung dieser Bereiche gelingt durch Konfigurationsstandards auf Ebene von iOS oder AppConfig, so

dass die bMD-Lösung auch für die komfortable Verteilung und Einrichtung der MCM-Funktionen sorgt, deren inhaltlichen Funktionen wie Datensynchronisation zu ausgewählten Backend-Systemen und Datenvisualisierung/-bearbeitung jedoch den Drittanbieter-Apps vorbehalten bleibt. Mit diesem Best-Of-Breed-Ansatz fügt sich MDM/MAM mit MCM zu einer umfassenden EMM-Lösung zusammen. Folgendes Diagramm soll diese Zusammenhänge anhand typischer Mechanismen verdeutlichen.



MDM + MAM + MCM = EMM

Der **Administrator** nutzt die MDM- und MAM-Features von baramundi Mobile Devices, um zunächst die Mobilgeräte der Mitarbeiter zu konfigurieren und abzusichern und dann die Business-Apps zu installieren und zu konfigurieren. Die spezifischen MCM-Funktionalitäten bringen dann entsprechende Apps von Drittanbietern mit, die ebenfalls per baramundi Mobile Devices verteilt und dabei gleich geeignet konfiguriert werden. Eine solche Konfiguration umfasst die Vorbelegung von Benutzernamen, Verbindungspfade zu Serversystemen und viele weitere Detaileinstellungen der Apps.

Im Falle eines Geräteverlusts hat der Administrator im Zusammenspiel mit geeigneten Apps die Möglichkeit, aus der Ferne gezielt die Daten in der App zu löschen (auch bekannt als „Enterprise Wipe“ oder „Selective Wipe“). Diese Funktion erleichtert die Implementierung von BYOD-Konzepten.

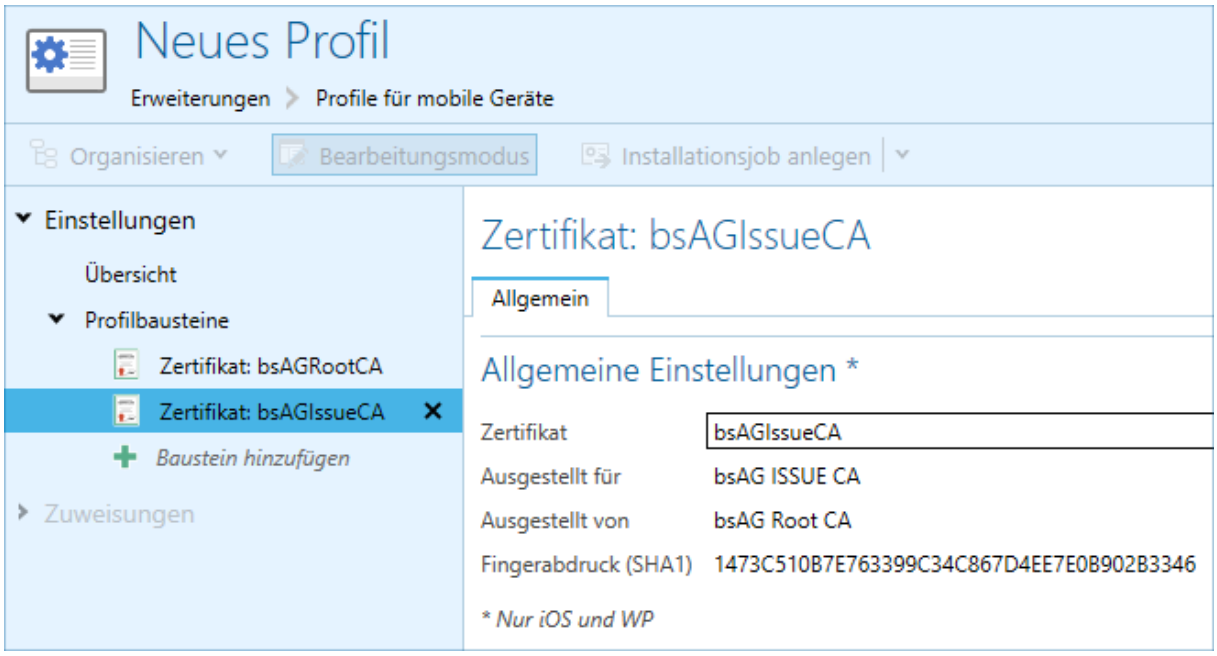
Der **Benutzer** kann auf seinem Gerät neben den Bordmitteln des Betriebssystems spezielle Container-Apps für PIM (Personal Information Management, d.h. E-Mails, Kalender, Kontakte, …) oder Dokumentenmanagement nutzen, die neben der Visualisierung der Inhalte auch die

Synchronisation mit Backend-Systemen bewerkstelligen. Derartige Apps liefern neben den Funktionalitäten je nach Ausprägung auch zusätzliche Sicherheitsfeatures, um dortige Daten zu verschlüsseln und im BYOD-Kontext geschäftliche Daten von privaten Daten getrennt zu halten.

Die **Fachabteilungen** (dazu zählt auch der o.g. Mobilgerätbenutzer) nutzen weiterhin deren vertraute Anwendungen, um Inhalte in den Unternehmenslösungen abzulegen. Mit Unternehmenslösungen sind dabei PIM-Systeme wie Microsoft Exchange bis hin zu Dateiablageorte wie SharePoint, WebDAV und diverse Cloud-Ablagen für Unternehmen gemeint.

2.9 Sicherheit durch Zertifikate, Verteilung und Enterprise Wi-Fi

Ferner sollte eine EMM-Lösung die Verteilung von Client-Unternehmenszertifikaten ermöglichen und die dafür nötigen Vertrauensstellungen (trust chains) gegenüber Unternehmensdiensten unterstützten können.



Profilbaustein für Clientzertifikate

Mittels solcher Zertifikate können dann Zugriffe auf Microsoft Exchange abgesichert werden oder das WLAN in Form eines sicheren Enterprise Wi-Fi implementiert werden. Beides sichert die Verbindung per Zertifikat anstelle von Benutzer-Credentials.

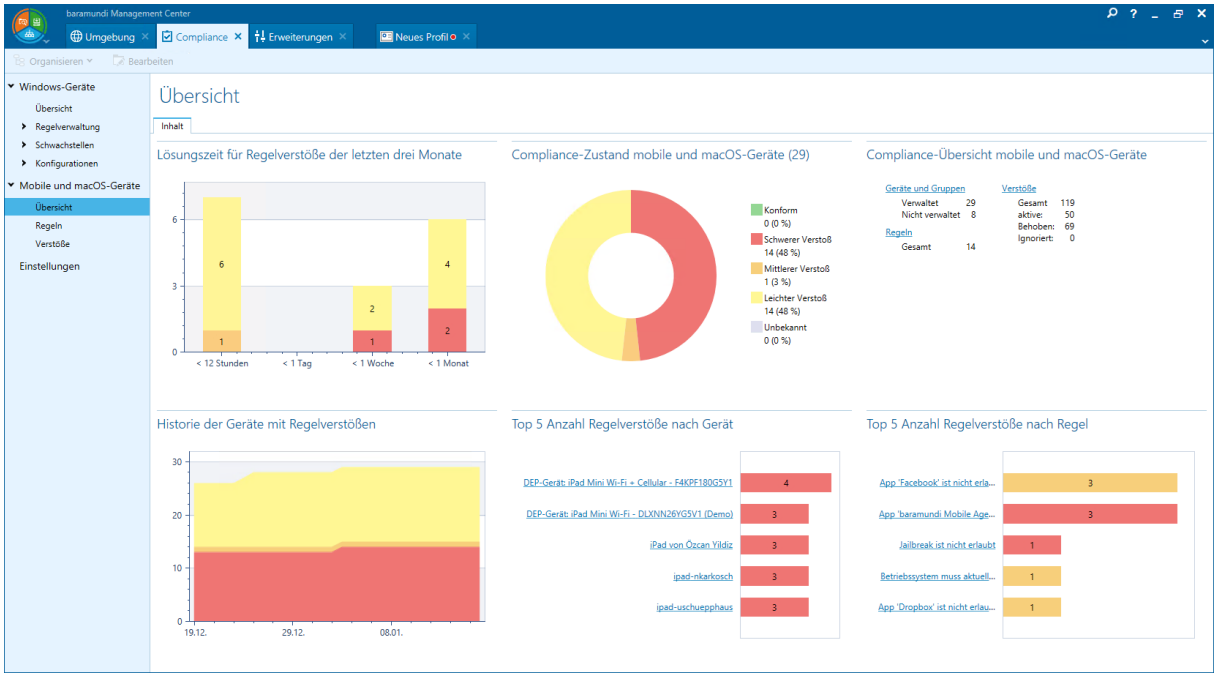
2.10 IT-Compliance prüfen

Gerade bei mobilen Geräten ist es besonders wichtig, die „IT-Compliance“ mit Unternehmensregeln sicherzustellen. Mithilfe von App-Black- und Whitelisting oder dem

Erkennen von Jailbreaks bzw. Roots lassen sich Vorgaben zur Sicherheit durchsetzen. So sollte die EMM-Lösung beispielsweise erkennen, wenn bestimmte als nötig festgelegte Apps auf dem Gerät fehlen.

Die Informationen zum Compliance-Stand sollten auf einem Dashboard übersichtlich angezeigt werden – sortiert nach Geräten oder Schwere der Verstöße. Auf einen Blick ist dann für den Administrator klar, wo akuter Handlungsbedarf besteht. Empfehlenswert sind EMM-Lösungen, die zudem automatisierte Reaktionen ermöglichen – von der E-Mail an den Nutzer bis hin zum Remote Wipe eines Gerätes bei besonders schwerwiegenden Verstößen, etwa einem Jailbreak.

Mit der baramundi Management Suite ist es auch möglich, dem Nutzer im Self-Service-Bereich die Möglichkeit zu geben, selbst den Compliance-Status des eigenen Smartphones oder Tablets abzurufen.



Dashboard für IT-Compliance

2.11 Self-Service-Möglichkeiten anbieten

Self-Service-Lösungen sind eine elegante Möglichkeit, dem Nutzer eine unmittelbare Unterstützung zu bieten und gleichzeitig das Aufkommen an Supportanfragen zu verringern. Dazu werden vorbereitete Administrationsjobs im Kiosk angeboten, die bei Abruf durch den Nutzer vollautomatisch und ohne Eingriffe eines Administrators ablaufen. Dadurch können Anwender beispielsweise selbständig Store-Apps und Unternehmens-Apps installieren bzw.

werden zur entsprechenden App im Store geführt. Auch Konfigurationseinstellungen können so angeboten werden.

2.12 Apple Device Enrollment Program (DEP)

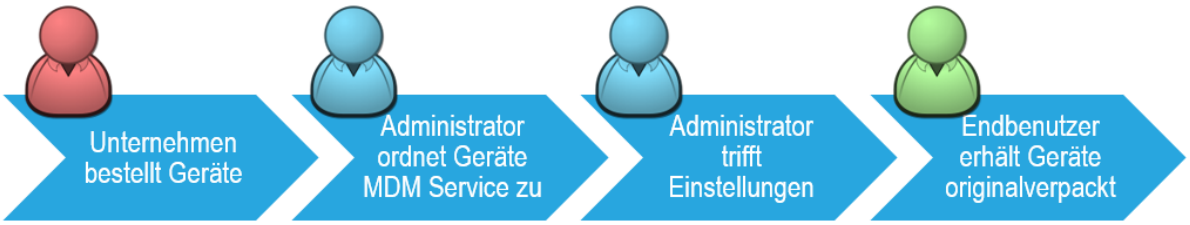
Apple stellt mit Einführung des Device Enrollment Program (DEP) effiziente Möglichkeiten bereit, um neue iOS-Geräte schnell und elegant in das Management einer EMM-Lösung aufzunehmen.

Es empfiehlt sich, eine EMM-Lösung auszuwählen, die diese Möglichkeiten unterstützt und so das unmittelbare Enrollment erlaubt. Der Administrator kann diesen Prozess per Konfiguration an die eigenen Präferenzen anpassen, indem er die Freiheitsgrade des Endbenutzers während der Aktivierungsphase des Geräts entsprechend definiert.

Die Vorteile von DEP für den Endbenutzer liegen in der schnelleren und einfacheren Aktivierung des Geräts. Das Unternehmen profitiert durch einen Zugewinn an Sicherheit: Der Administrator stellt durch neue Einstellungen sicher, dass ein Unternehmensgerät immer gemanagt wird. Insbesondere kann er verhindern, dass Management-Profile von iOS-Geräten durch den Endbenutzer entfernt werden.

2.12.1 Der DEP-Bereitstellungsprozess

Durch Apples DEP sind folgende vereinfachte Bereitstellungsprozesse innerhalb einer EMM-Lösung möglich, die die Einrichtung beschleunigen und so auch elegantes Massen-Enrollment bieten.



Bereitstellungsprozess für iOS-Geräte

Das Unternehmen bestellt die iOS-Geräte bei Apple oder einem für DEP-autorisierten Händler bzw. Telefonieanbieter. Noch vor der Auslieferung werden die Geräte dem EMM-Service durch den Administrator zugeordnet und Konfigurationseinstellungen in der EMM-Lösung getroffen. Der Endbenutzer erhält so die Geräte originalverpackt mit sofortiger Managementanbindung bereits zum Zeitpunkt der Geräteaktivierung.

2.12.2 DEP aus Sicht des Administrators

Der Administrator benötigt auf das iOS-Gerät keinen physischen Zugriff mehr, um das Gerät sicher in das Enterprise Mobility Management einzubinden.

Mit einer EMM-Lösung kann er das neue Gerät vorkonfigurieren, um im Zuge der Aktivierung bereits die Unternehmens-richtlinien sicherzustellen. Somit kann er verhindern, dass der Benutzer das Gerät wieder aus dem Management entfernt, und erreicht, dass alle Benutzer die gleiche Gerätekonfiguration erhalten.

Innerhalb eines einfachen Profils definiert der Administrator die gewünschten Eigenschaften und Freiheitsgrade des Endbenutzers während der Aktivierung.

iOS Device Enrollment Profile

2.12.3 DEP aus Sicht des Endbenutzers

Für den Endbenutzer vereinfacht sich dank DEP der Aktivierungsprozess eines neu erhaltenen iOS-Geräts spürbar. Anstelle einer Vielzahl von Dialogseiten, die der Benutzer bisher im Zuge der Aktivierung beantworten musste, erhöht nun die Vorkonfiguration des Administrators den Automatisierungsgrad.

Durch geeignete Vorkonfiguration werden dem Benutzer Fragen abgenommen und die Sicherheit erhöht. Diese Vereinfachung betrifft nicht nur die Erstinbetriebnahme, sondern trifft auch bei der Installation von Apps zu, da in Verbindung mit VPP (s.u.) ohne lästige Rückfragedialoge die gewünschten Apps den Weg auf das Gerät finden.

iOS-Aktivierung mit DEP

2.13 Apple Volume Purchase Program (VPP)

Für Unternehmen entwickelt Apple das Volume Purchase Program (VPP) zum Einkauf und zur Verwaltung von App-Lizenzen kontinuierlich weiter und bietet dem Administrator parallel alternative Nutzungsmöglichkeiten. Die EMM-Lösung sollte daher neben dem App-Einkauf per VPP Redemption Codes auch die App-Verteilung per Managed Distribution Client Assignment unterstützen. Somit lassen sich Lizenzen für Geräte kaufen und diesen zuordnen, anstatt Lizenzen an Apple-IDs von Benutzern koppeln zu müssen.

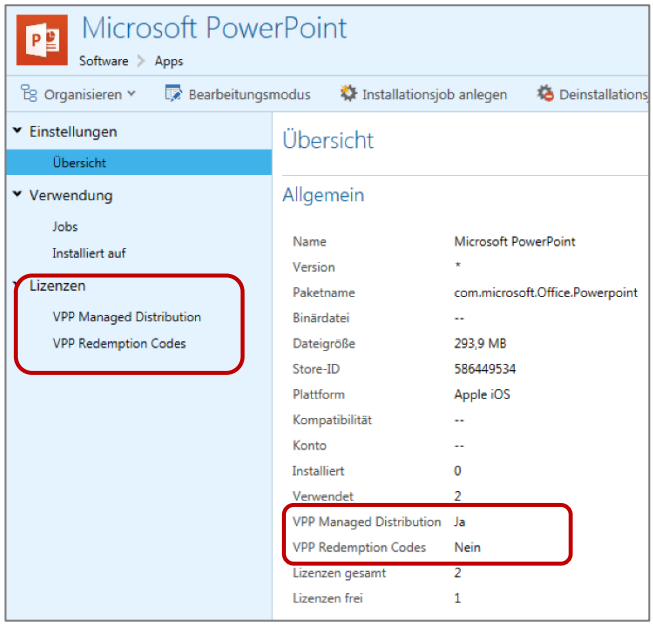
	VPP Redemption Codes	VPP Managed Distribution User Assignment	VPP Managed Distribution Client Assignment
Verknüpfung der Lizenzen	Apple ID*	Apple ID*	Gerät
Verteilung kostenloser und -pflichtiger Apps	nur **mit** Apple ID*	nur **mit** Apple ID*	**ohne** Apple ID*
Verteilung ohne Benutzerinteraktion	n/a	n/a	ja (für supervised Geräte)
Handling der Lizenzen / Anzeige in MDM-Suite	Listen von Lizenzen; manuelle Eingabe	automatische Assoziation in der MDM-Suite	automatische Assoziation in der MDM-Suite
Zurückziehen von Lizenzen durch den Administrator	n/a	ja	ja
Verfügbarkeit seitens Apple	iOS 5	iOS 7	iOS 9

*) „Apple ID“ bezeichnet die ID des Endbenutzers gegenüber Apple

2.13.1 VPP-Unterstützung aus Sicht des Admins

Die VPP-Unterstützung bietet verschiedene Möglichkeiten bei der Verteilung kostenpflichtiger und kostenfreier Apps. Der Administrator kann dazu beliebig zwischen dem Einsatz von Redemption Codes oder Managed Distribution wählen, individuell für jede App.

Werden die Lizenzen einem Gerät zugewiesen, so können diese auch wieder entzogen werden, um sie für ein anderes Gerät wiederzuverwenden.



VPP Unterstützung in bMD

3 Umfassend, effizient und einfach

3.1 Integriert vs. Standalone: Was eignet sich für wen?

Eine grundlegende Entscheidung betrifft die Art der Einbindung der Lösung in die bestehende Unternehmens-IT. Zur Auswahl stehen EMM-Lösungen, die in eine Unified-Endpoint-Management(UEM)-Suite integriert sind, oder EMM-Standalone-Lösungen. Unternehmen, die sich für eine UEM-Software entscheiden, können damit häufig auch mobile Geräte verwalten. Der Vorteil hierbei liegt auf der Hand: Ist das EMM in das Unified-Endpoint-Management integriert, dann lassen sich alle Clients zentral über eine Oberfläche managen und der Administrator hat einen Gesamtüberblick. Das eignet sich besonders dann für Unternehmen, wenn ein oder nur wenige IT-Administratoren für die IT-Infrastruktur verantwortlich sind und dadurch Synergieeffekte nutzen können. Auch wenn der Funktionsumfang im Vergleich zu reinen EMM-Suiten möglicherweise etwas kleiner ausfällt, werden in der Regel die wichtigsten Funktionen wie beispielsweise Inventarisierung, Konfigurationsmöglichkeiten sowie die Verteilung von Apps und Sicherheitseinstellungen abgedeckt.

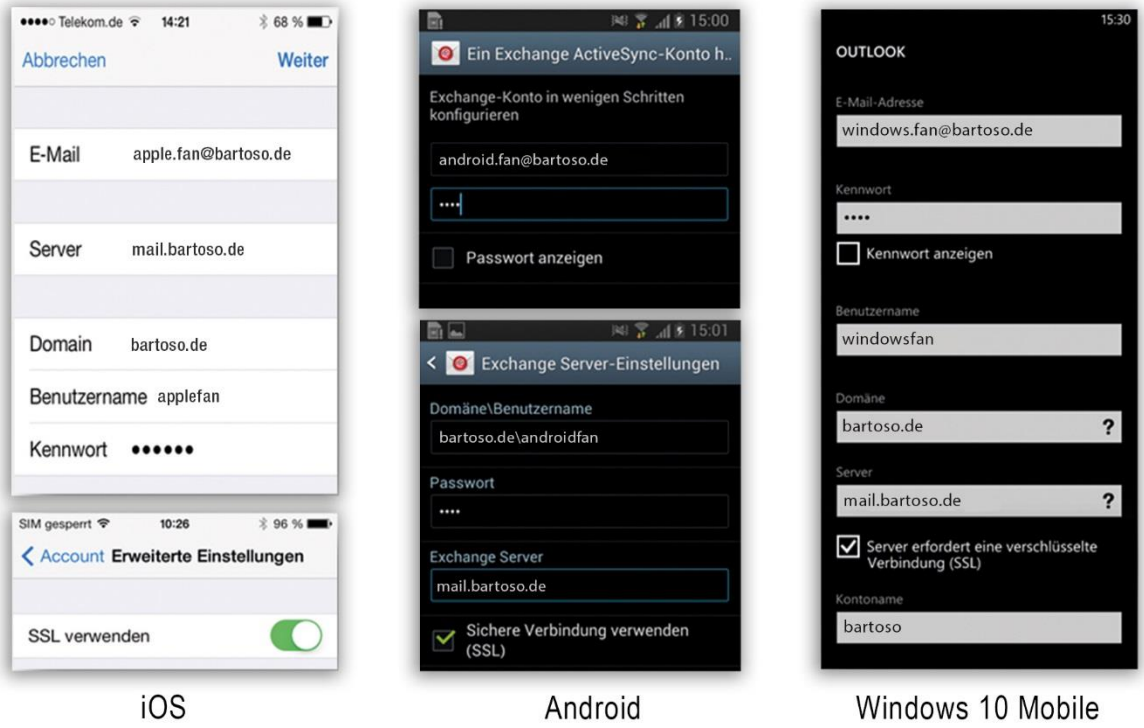
3.2 Implementierungsaufwand und Bedienbarkeit einer Lösung

Bei der Entscheidung für eine EMM-Software sollten Administratoren berücksichtigen, wie hoch der Aufwand für die Implementierung, Inbetriebnahme und Schulung liegt. Die Suite sollte möglichst einfach in die bestehende IT-Landschaft integriert werden können. Darüber hinaus ist wichtig, dass die Lösung intuitiv zu bedienen ist und eine übersichtliche Oberfläche bietet. So können auch neue Kollegen oder eine Vertretung schnell in die Handhabung der EMM-Suite eingewiesen werden. Ein weiteres Plus: Umfangreiche Schulungen verursachen zusätzliche Kosten – und gerade IT-Abteilungen müssen mit den oft knappen Budgets sinnvoll wirtschaften.

3.3 Herausforderung der Plattformvielfalt

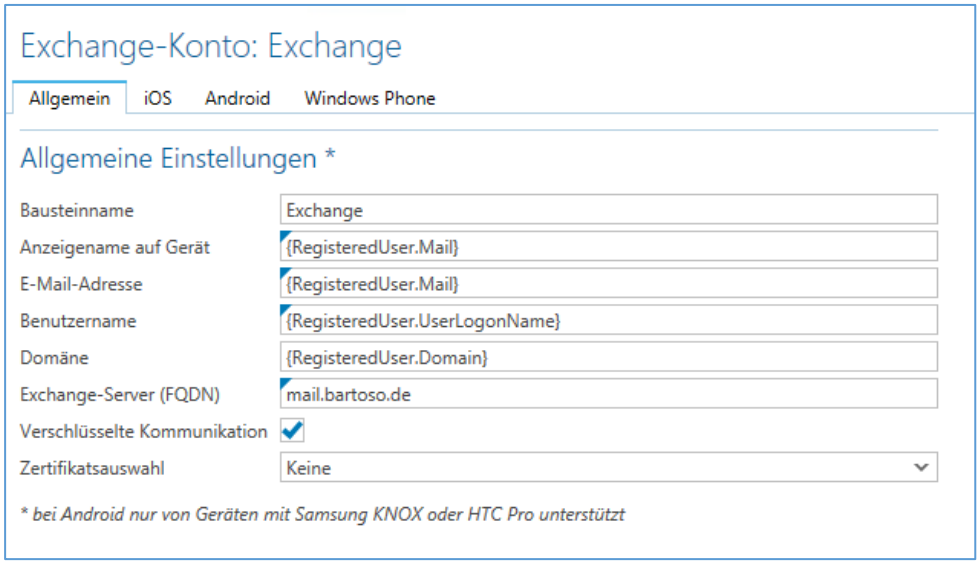
Administratoren sind häufig gefordert, verschiedene Mobilplattformen zu unterstützen, d.h. bis in die Konfigurationsdetails zu verstehen, einzurichten und zu unterstützen. Das ist nicht nur komplex, sondern infolgedessen auch zeitaufwändig.

Am Beispiel der Exchange-Konfiguration zur Bereitstellung von E-Mail-Empfang auf den drei populären Mobilplattformen Android, iOS und Windows Mobile zeigt sich deutlich, wie stets die gleichen Parameter (Name, E-Mail-Adresse, Domäne, Server, Verschlüsselung) in unterschiedliche Dialoge einzugeben sind, sofern das von Hand geschieht.



Exchange-Konfiguration auf verschiedenen Mobilplattformen

Der Wunsch nach einem Werkzeug, das eine einheitliche Eingabe für alle zu verwaltenden Geräte ermöglicht, liegt somit auf der Hand. Mit einer Enterprise-Mobility-Management-Lösung wie der baramundi Management Suite kann der Administrator über eine Oberfläche alle Mobilgeräte einheitlich verwalten. Damit lässt sich beispielsweise eine Exchange-Konfiguration für verschiedene Betriebssysteme einfach und schnell bewerkstelligen.



Plattformübergreifende Exchange-Konfiguration mittels EMM-Suite

3.4 Transparentes Management in Echtzeit

Eine gute EMM-Software stellt nicht nur alle relevanten Daten zu den verwalteten Mobilgeräten übersichtlich bereit, diese sollten möglichst in Echtzeit zur Verfügung stehen. Denn nur wenn der Administrator alle für ihn wichtigen Informationen und Rückmeldungen zeitnah erhält, ist er ausreichend informiert und kann so die Sicherheit der Mobilgeräte korrekt beurteilen. Job-orientierte Mechanismen punkten hierbei gegenüber regelbasierten Paradigmen. Steht eine jederzeit aktuelle Datenbasis bereit, lassen sich damit bei Bedarf aktuelle Reports exportieren und aufbereiten.

4 Checkliste wichtiger Funktionen

	Softwareverteilung und Konfiguration
☐	Verteilung Firmware-Updates
☐	Installation von Apps mit | ohne Benutzerbestätigung
☐	Deinstallation von Apps mit | ohne Benutzerbestätigung
☐	Support für Apple Volume Purchase Program (VPP)
☐	Support für Apple Device Enrollment Program (DEP)
☐	Installation | Deinstallation bei deaktiviertem App Store
☐	Installation | Deinstallation selbsterstellter Unternehmens-Apps
☐	Self-Service-App: Kiosk
☐	Installation | Deinstallation von Zertifikaten
☐	Parametrisierung von Einstellungen über Variablen
☐	Installation von Hyperlinks (iOS: Web Clip)
☐	Deaktivierung der Kamera
☐	Konfiguration von Access Points (APN)
☐	VPN Einstellungen

	Inventarisierung
☐	Hardwareinformationen
☐	Konfigurierte Einschränkungen (iCloud Sperre u.ä.)
☐	Installierte Profile
☐	Installierte Zertifikate
☐	SIM-Informationen
☐	Roaming Status
☐	Sicherheitseinstellungen
☐	Letzter Kontakt
☐	Gruppierung Geräte

	Sicherheit
☐	Remote Lock | Unlock | Wipe
☐	Festlegung PIN-/Passwortabfrage und -komplexität
☐	Erkennung von Firmware-Manipulationen (Jailbreak, Root)
☐	Richtlinien f. Geräteverschlüsselung setzen
☐	Unterstützung Whitelist | Blacklist für Apps
☐	Deaktivierung von System-Apps
☐	Deaktivierung WLAN
☐	Deaktivierung Bluetooth
☐	Passwort History | Reset | Neues Passwort setzen
☐	Zugriff auf SD-Karte zulassen / nicht zulassen

☐	Zugriff auf App Stores zulassen / nicht zulassen
☐	WLAN auto-connect

	Compliance
☐	Fehlen von erforderlichen Apps erkennen
☐	Installation von unerwünschten Apps erkennen
☐	Erkennung falsche Konfiguration
☐	Erkennung veralteter Betriebssystemversionen
☐	Status und Historie von Regelverstößen

5 Fazit

Bei der Wahl einer EMM-Lösung gibt es nicht die eine Lösung, die für alle Unternehmen optimal passt. Wichtig ist, den Funktionsumfang genau zu definieren und passende Lösungen zu testen. Neben den gebotenen Funktionalitäten spielen auch die Art des Betriebs wie die Handhabung der Lösung eine entscheidende Rolle. Doch neben der Technik müssen auch die Mitarbeiter abgeholt werden, denn ohne deren Akzeptanz ist das gesamte Mobility-Projekt zum Scheitern verurteilt. Aus diesem Grund sollten IT-Verantwortliche bei der Wahl einer EMM-Lösung auch immer im Blick haben, dass ein ausgewogenes Verhältnis vorherrscht zwischen den Sicherheitsanforderungen des Unternehmens, der Akzeptanz der Mitarbeiter bei der Nutzung der Mobilgeräte und der einfachen Bedienung der Managementmöglichkeiten durch den Administrator. Denn nur wenn allen drei Punkten Rechnung getragen wird, ist die Einführung einer EMM-Lösung ein Erfolg.

Über die baramundi software AG

Die baramundi software AG ermöglicht Unternehmen und Organisationen das effiziente, sichere und plattformübergreifende Management von Arbeitsplatzumgebungen. Mehr als 2.500 Kunden aller Branchen und Größen profitieren weltweit von der langjährigen Erfahrung und den ausgezeichneten Produkten des deutschen Herstellers. Diese sind in der baramundi Management Suite nach einem ganzheitlichen, zukunftsorientierten Unified-Endpoint-Management-Ansatz zusammengefasst: Client-Management, Mobile-Device-Management und Endpoint-Security erfolgen über eine gemeinsame Oberfläche, in einer einzigen Datenbank und nach einheitlichen Standards.

Durch die Automatisierung von Routinearbeiten und eine umfassende Übersicht über den Zustand aller Endgeräte optimiert die baramundi Management Suite Prozesse des IT-Managements. Sie entlastet die IT-Administratoren und sorgt dafür, dass Anwendern jederzeit und überall die benötigten Rechte und Anwendungen auf allen Plattformen und Formfaktoren zur Verfügung stehen – auf PCs, Notebooks, Mobilgeräten oder in virtuellen Umgebungen.

Der Firmensitz der baramundi software AG befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in Germany. Beim Vertrieb, der Beratung und Betreuung von Anwendern arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

Mehr Informationen zu baramundi: www.baramundi.de

Sie möchten sich die EMM-Lösung ansehen? Melden Sie sich zum Live-Webinar an

Erleben Sie, wie Sie Smartphones und Tablets genauso einfach und zuverlässig verwalten wie PCs und Notebooks: www.baramundi.de/webinar

baramundi

Wir freuen uns Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software AG
Beim Glaspalast 1
86153 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.de
www.baramundi.de

+44 2071 93 28 77
request@baramundi.co.uk
www.baramundi.co.uk

+48 735 91 44 54
request@baramundi.pl
www.baramundi.pl

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
550 Cochituate Road, Suite 25
Framingham, MA 01701, USA

+1 508 861 75 61
requestUSA@baramundi.com
www.baramundi.com

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

+43 1 7 17 28 - 545
request@baramundi.at
www.baramundi.at

Empower your IT