

# IT-BUSINESS

## SPEZIAL

Verlags-Sonderveröffentlichung 24/2014

### Endpoint & Mobile Security

> MDM

> Authentication

> Verschlüsselung

> BYOD

> Passwort

> NAC

> IAM

> Schwachstellen-Management



# MOBIL, EINFACH, SICHER

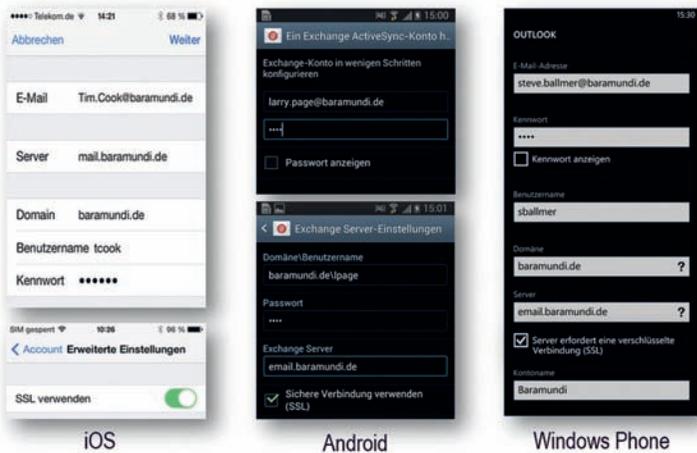
## Smartphones und Tablets plattformübergreifend konfigurieren

Die Konfiguration von Smartphones und Tablets ist für IT-Administratoren sehr aufwändig. Dieselben Einstellungen müssen auf Geräten mit verschiedenen mobilen Betriebssystemen vorgenommen werden. Eine zentrale, plattformübergreifende Konfiguration der Geräte sorgt für Abhilfe.

baramundi bietet zentrales und automatisiertes  
Mobile-Device-Management

Sie sind wesentlich handlicher als Notebooks, und immens praktisch: Smartphones und Tablets erlauben als mobile Alleskönner eine schnelle Antwort auf eine E-Mail-Anfrage vom Bahnsteig oder eine schnelle Recherche im Internet aus dem Zugabteil. Für IT-Administratoren hat die Sache allerdings einen Haken: Sie müssen in der Regel mehrere Mobilplattformen unterstützen, die Geräte einrichten und sicher konfigurieren. Dies verursacht zusätzlich zum Management der bekannten Windows-Systeme Komplexität und ist zeitaufwändig.

**Konfiguration von Mobilgeräten: Plattformübergreifend statt aufwändig.** Ein Vergleich der drei populären Mobilplattformen iOS, Android und Windows Phone zeigt, dass dieselben Parameter (Name, E-Mail-Adresse, Domäne, Server, Verschlüsselung) an unterschiedlichen Stellen eingegeben werden müssen. Das bedeutet: Der Administrator muss die entsprechenden Eingabemaschen auf allen



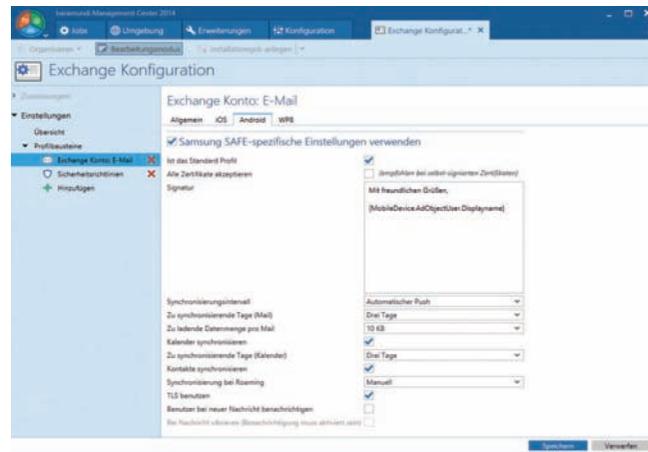
Exchange-Konfiguration auf verschiedenen Mobilplattformen

Geräten kennen und verstehen, bei der Konfiguration aufrufen und ausfüllen. Dieser Workflow lässt sich durch die Verwendung plattformübergreifender Profilbausteine und eine zentrale Verwaltung der Geräte stark vereinfachen.

**Das Smartphone oder Tablet** muss dazu einmal in die Verwaltungslösung aufgenommen werden („Enrollment“), zum Beispiel durch das Scannen eines bereitgestellten Barcodes. Anschließend können Management-Aufgaben – am Beispiel der hier abgebildeten Screenshots zu Exchange-Konfigurationen – über die Lösung zentral durchgeführt werden. Auf einer einheitlichen, plattformübergreifenden Oberfläche werden die entsprechenden

Einstellungen gesetzt und können anschließend auf das verwaltete Gerät übertragen werden.

**Die Vorteile liegen auf der Hand:** Der Administrator muss nicht mehr wissen, wo auf



Einheitliche Oberfläche für die Exchange-Konfiguration in der Management Suite von baramundi

welchem Mobilgerät welche Einstellung vorgenommen wird – er nutzt stets die bekannte Oberfläche seiner zentralen Management-Konsole. Das verringert die Komplexität, spart Zeit und reduziert die Fehleranfälligkeit des Prozesses. Damit ergibt sich unterm Strich auch ein Mehr an Sicherheit.

**Ein weiterer Vorteil:** Management-Aufgaben lassen sich über eine Verwaltungs-Soft-

ware auch „remote“ durchführen, ohne dass ein Administrator das Gerät in die Hand nehmen muss. Nimmt ein Nutzer beispielsweise an einem Außenstandort ein neues Handy in Betrieb, scannt er einfach den Barcode, den ihm der Administrator aus der Zentrale per E-Mail zugesendet hat, anschließend kann dieser die weitere Konfiguration vornehmen. Die verwendeten Abläufe und Aufgaben lassen sich vorbereiten und immer wieder verwenden – auch für eine größere Anzahl von Geräten gleichzeitig oder zeitgesteuert.

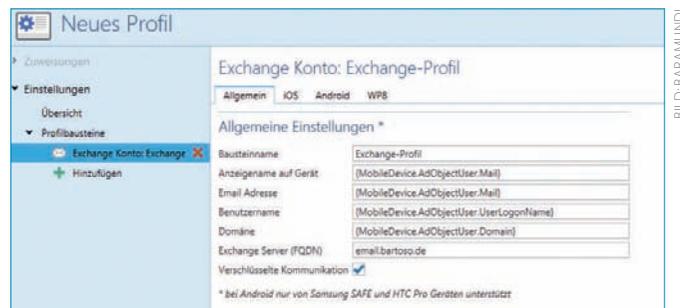
**Die richtige Konfiguration eines Mobilgerätes** ist nicht nur für ein reibungsloses Arbeiten wichtig: Ein handliches Smartphone oder Tablet geht schnell verloren oder könnte gestohlen werden. Dagegen gilt es ebenfalls Vorkehrungen zu treffen, zum Beispiel durch ein starkes Passwort und eine automatische Sperre beim Ausschalten des Bildschirms oder eine Möglichkeit zum „Remote Wipe“. Zudem muss der IT-Administrator die Geräte im laufenden Betrieb im Auge behalten, damit nicht versehentlich oder vorsätzlich wichtige Einstellungen vom Nutzer verändert werden – schließlich hat der Endanwender auf Mobilgeräten in der Regel volle Administrationsrechte.

**Gute Lösungen für Mobile-Device-Management**

bieten daher die Möglichkeit, Compliance-Regeln zu definieren, die auf den Geräten regelmäßig geprüft werden. Verstöße werden dem Administrator übersichtlich angezeigt. Damit ist eine schnelle, gezielte Reaktion möglich, um wieder einen sicheren Zustand herzustellen, von der E-Mail an den Nutzer über eine automatisierte Aktion auf dem Gerät bis hin zum Komplett-Löschen aus der Ferne.

**Im Idealfall ist das Mobile-Device-Management** in eine Software-Suite für Client-Management integriert. Das spart nicht nur Aufwand bei der Einrichtung, bei der Wartung und der Bedienung. Es ermöglicht darüber hinaus, Mobilgeräte und PCs in gemeinsamen Gruppen und Organisationseinheiten zu verwalten und Standards durchzusetzen. Dieser Ansatz gilt zudem als zukunftssicher: Neue Geräteklassen lassen sich in eine einheitliche Lösung leichter einbinden.

[<http://www.baramundi.de/mdm-uebersicht>]



Übersicht über Regelverstöße und Compliance-Status in der Management Suite von baramundi