



DNUG 11.2010

UC 2

iPhone & iPad im Unternehmenseinsatz

Dipl.-Ing. Detlev Pöttgen



Über mich – Detlev Pöttgen



dp consulting | purify it  
<http://www.dpocs.de>

Lotus Notes Traveler

- Infrastruktur & Security Workshops
- Traveler Rollouts bei diversen Kunden
- Größte Kundenumgebung:
  - 700 aktive Devices
  - Nokia, Windows Mobile, Apple & Android
- Entwicklung von Tools rund um Traveler  
(Administration & Apple Device Enrollment)

IBM Design Partner for Domino Next  
Apple Enterprise Developer Program

Blog: <http://www.netzgoetter.net>

2

Agenda 

**Worum geht es in dieser Session?**

**iPhone & iPad im Unternehmenseinsatz**

-  - Warum wir uns damit beschäftigen müssen?
-  - IBM Lotus Notes Traveler auf iOS Geräten
-  - iOS Enterprise Funktionen
-  - Over-the-Air-Deployment & MDM

3

Die Sinn Frage? 



4

Die Sinn Frage?



### iPod touch

Leistungsmerkmale Design iOS 4 Spiele + Apps Galerie Technische Daten Jetzt kaufen

## Was für eine Spieltechnik.

Der iPod touch ist das beliebteste mobile Spielgerät der Welt. Im App Store sind tausende Spiele und andere Apps in allen möglichen Kategorien nur einen Fingertipp entfernt. Damit hat der iPod touch mehr Spiele als jede andere Plattform. Du wirst dir wünschen, mehr Finger zu haben.



A4 Chip



Retina Display



Game Center



5

Die Sinn Frage?



### iPhone in Unternehmen

Businessfunktionen Integration Apps fürs iPhone Praxisberichte

## Axel Springer



iPhone in Aktion.  
Video ansehen >



Dir Deine Meinung!

### Mobile Inhalte auf dem iPhone.

Der europäische Verlagsriese Axel Springer ist weitaus mehr als nur ein gigantisches Printunternehmen - man hat sich dort auch das Ziel gesetzt, das kreativste und profitabelste Multimediaunternehmen Europas zu werden. Zu diesem Zweck hat sich das Unternehmen von einem traditionellen Verlag in einen der größten Anbieter für digitale Medien verwandelt. Die Entscheidung des Axel Springer Verlags, für die Übermittlung mobiler digitaler Inhalte das Apple iPhone 3G einzusetzen, ist dabei ein wichtiger Schritt.



6

Die Sinn Frage?



7

Warum muß ich mich damit beschäftigen?



8

Warum muß ich mich damit beschäftigen?



9

Warum muß ich mich damit beschäftigen?



Fakt bei vielen Kunden:  
Ich habe iOS Geräte, um die ich kümmern muß.  
Spätestens wenn es heißt wie bekomme ich meine Mails auf das Gerät.

10

Warum muß ich mich damit beschäftigen?



Oft wird das Gerät der IT in die Hand gegeben und das notwendige manuell eingerichtet (WLAN, VPN, Traveler...).

Kümmert sich jemand um die Sicherheit?



11

Warum muß ich mich damit beschäftigen?



Ich habe iOS Geräte, dann muß ich auch

- Step 1: Gerätestandards (Policys) definieren
- Step 2: Policys in Konfigurationen umsetzen
- Step 3: Device Enrollment
- Step 4: Überwachung & Steuerung aktiver Devices



12

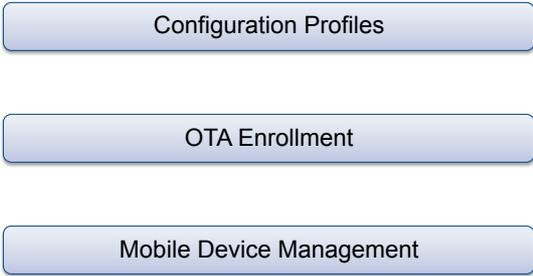
Warum muß ich mich damit beschäftigen?



- Step 1: Geräte Policys definieren
- Step 2: Policys in Konfiguration umsetzen  
**Configuration Profiles**
- Step 3: Device Enrollment  
**OTA Enrollment**
- Step 4: Management aktiver Devices  
**Mobile Device Management**



13



14

## IBM Lotus Notes Traveler auf iOS Geräten



Unumgänglicher Schritt:  
iPhone-Aktivierung per iTunes (im Aktivierungsmodus)



Details: **iPhone Enterprise Deployment Guide Kapitel 4**

[http://manuals.info.apple.com/en\\_US/Enterprise\\_Deployment\\_Guide.pdf](http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf)



15



Configuration Profiles

OTA Enrollment

Mobile Device Management



16

## Configuration Profiles & Traveler



---



Apple unterstützt eine Profil basierte Konfiguration

- XML Dateien (plist DTD)
- Endung .mobileconfig

Beinhalten eine oder mehrere Device-Einstellungen (sogenannte Payloads):

- Exchange Traveler, IMAP, POP Accounts
- Zertifikate, VPN, WLAN
- Passcode, Einschränkungen, ...

Erzeugt werden Profile durch:

- iPhone Configuration Utility
- Eigene Scripte
- Drittanbieter Management Lösungen



17

## IBM Lotus Notes Traveler auf iOS Geräten



---



Die Traveler –Einrichtung erfolgt durch solch ein Apple Profil.

Es wird keine eigene App auf dem iOS Gerät installiert, sondern die integrierte ActiveSync Komponente verwendet.

Diese wird mit Apple-Mitteln per Profile mit einem „Exchange“ Payload konfiguriert.



18

## IBM Lotus Notes Traveler auf iOS Geräten



Der Endbenutzer geht auf dem Endgerät per Browser auf die Traveler Startseite ( <https://host/servlet/traveler> ) und wählt die Bootstrap Datei aus, welche das Konfigurationsprofil darstellt.



19

## IBM Lotus Notes Traveler auf iOS Geräten



IBM nutzt die von Apple zur Verfügung gestellten Sicherheitsfunktionen und integriert sich komplett in das Deployment-Konzept von Apple.

Mit den Traveler Sicherheitseinstellungen kann ich einige Sicherheits-Vorgaben bereits erfüllen.

- Passcode
- Wipe eines Geräts bei Diebstahl oder falscher PIN
- Sichere komplexe PIN
- Deaktivierung der Kamera
- Prüfung ob Vorgaben erfüllt sind und nur dann PIM-Daten zu lassen.



20

## IBM Lotus Notes Traveler auf iOS Geräten



Traveler allein deckt aber nicht alle Anforderungen für ein Enterprise Deployment ab.

Dafür ist es von der IBM nicht vorgesehen und dies kann nicht Aufgabe der IBM sein.

Will man die Einrichtung des iOS Gerätes weiter automatisieren, muß man sich im Detail mit den iOS Enterprise Funktionen beschäftigen.

Apple selbst bietet keinen eigenen Device Management Server an, sondern verweist hier auf Drittanbieter.



21

## iOS Enterprise Funktionen



Für kleine Umgebungen mit einigen Endgeräten wird aber noch nicht zwangsläufig eine komplexe Device Management Lösung benötigt.

Man hat dann aber auch keine automatische Over-the-Air-Lösung.

Apple bietet eine Windows und Mac basierte Anwendung an, mit der zentral Profile erstellt und diese **lokal (per USB)** auf Endgeräte verteilt werden können.

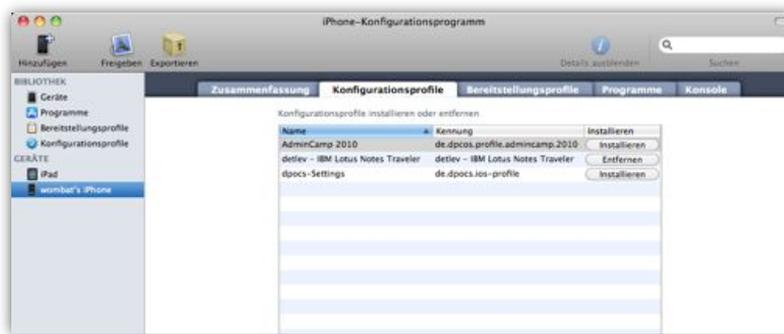
Das iPhone Configuration Utility kann kostenlos von der Apple Seite heruntergeladen werden.

<http://www.apple.com/support/iphone/enterprise/>



22

## iOS Enterprise Funktionen

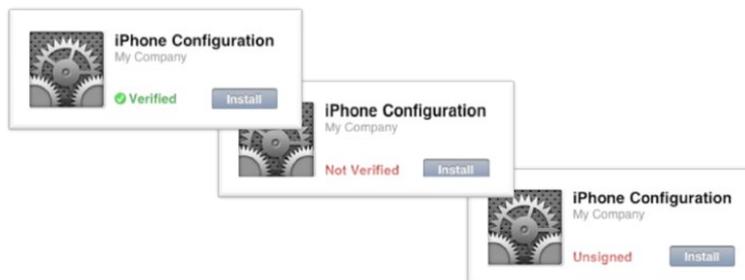


## iOS Enterprise Funktionen



Profile können:

- Per USB auf das verbundene Device übertragen werden.
- Exportiert & Verteilt werden
- Per Mail verschickt oder auf einem HTTP Server bereitgestellt werden
- Wichtig: Profile sollten signiert & verschlüsselt werden



iOS Enterprise Funktionen 

Profile Payloads

**Allgemein**  
Erforderlich

- Code**  
Nicht konfiguriert
- Einschränkungen**  
Nicht konfiguriert
- Wi-Fi**  
Nicht konfiguriert
- VPN**  
Nicht konfiguriert
- E-Mail**  
Nicht konfiguriert
- Exchange-ActiveSync**  
Nicht konfiguriert

- LDAP**  
Nicht konfiguriert
- CalDAV**  
Nicht konfiguriert
- CardDAV**  
Nicht konfiguriert
- Abonnierte Kalender**  
Nicht konfiguriert
- Webclips**  
Nicht konfiguriert
- Zertifikate**  
Nicht konfiguriert
- SCEP**  
Nicht konfiguriert
- Verwaltung mobiler Geräte**  
Nicht konfiguriert
- Erweitert**  
Nicht konfiguriert



iOS Enterprise Funktionen 

**Code (Passcode):**

Das sollten wir alles vom Traveler wiedererkennen.

Bei der Kennwortkomplexität nicht übertreiben.

Bei der Überschreitung der Anzahl der Fehlversuche wird das Gerät gelöscht.

**Allgemein**  
Erforderlich

**Code**  
1 Payload konfiguriert

**Code**

- Code-Eingabe auf Gerät erforderlich**  
Code muss eingegeben werden, bevor das Gerät verwendet werden kann
  - Einfache Werte erlauben**  
Wiederholende, aufsteigende und absteigende Zeichenfolgen erlauben
  - Alphanumerische Werte erforderlich**  
Benötigt Code mit mindestens einem Buchstaben
- Mindestlänge des Codes**  
Geringste zulässige Anzahl an Code-Zeichen:
- Mindestanzahl von komplexen Zeichen**  
Geringste zulässige Anzahl an nicht alphanumerischen Zeichen:
- Maximale Code-Gültigkeit (1-730 Tage oder Ohne)**  
Anzahl der Tage, nach denen der Code geändert werden muss:
- Automatische Sperre (1-5 Minuten oder Ohne)**  
Gerät bei Zeitüberschreitung automatisch sperren:
- Code-Verlauf (1-50 Codes oder Ohne)**  
Anzahl der eindeutigen Codes bis zur ersten Wiederholung:
- Zeitgrenze für Gerätespernung**  
Dauer, für die das Gerät gesperrt ist, ohne den Code für das Entsperren abzufragen:
- Maximale Anzahl von Fehlversuchen**  
Anzahl der erlaubten Code-Eingabeveruche, bevor alle Daten auf dem Gerät gelöscht werden:



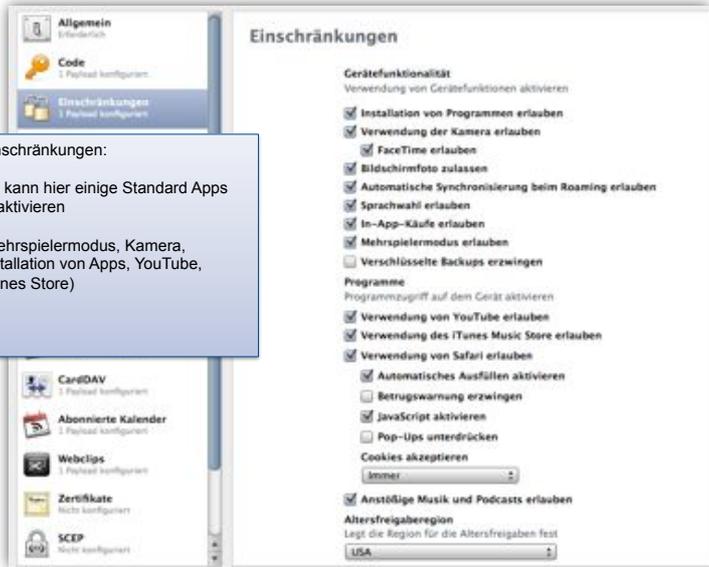


## iOS Enterprise Funktionen

**Einschränkungen:**

Ich kann hier einige Standard Apps deaktivieren

(Mehrspielermodus, Kamera, Installation von Apps, YouTube, iTunes Store)



The screenshot shows the 'Einschränkungen' (Restrictions) settings page. The left sidebar lists 'Allgemein', 'Code', 'Einschränkungen', 'CardDAV', 'Abonnierte Kalender', 'Webclips', 'Zertifikate', and 'SCEP'. The main content area is titled 'Einschränkungen' and includes sections for 'Gerätefunktionalität' (Device Functionality) and 'Programme' (Programs). Under 'Gerätefunktionalität', several options are checked, including 'Installation von Programmen erlauben', 'Verwendung der Kamera erlauben', 'FaceTime erlauben', 'Bildschirmfoto zulassen', 'Automatische Synchronisierung beim Roaming erlauben', 'Sprachwahl erlauben', 'In-App-Käufe erlauben', 'Mehrspielermodus erlauben', and 'Anstößige Musik und Podcasts erlauben'. Under 'Programme', 'Verwendung von YouTube erlauben', 'Verwendung des iTunes Music Store erlauben', and 'Verwendung von Safari erlauben' are checked. At the bottom, the 'Altersfreigaberegion' is set to 'USA'.



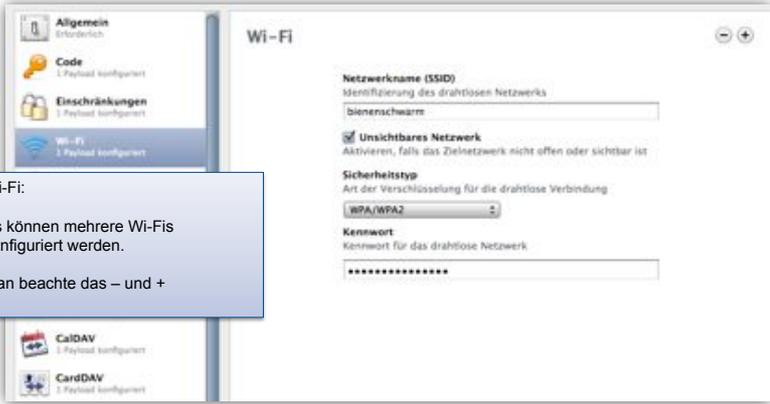


## iOS Enterprise Funktionen

**Wi-Fi:**

Es können mehrere Wi-Fis konfiguriert werden.

Man beachte das – und +

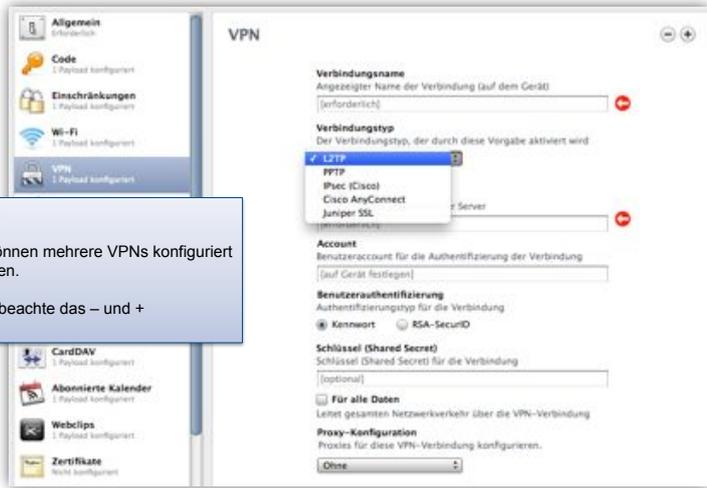


The screenshot shows the 'Wi-Fi' settings page. The left sidebar lists 'Allgemein', 'Code', 'Einschränkungen', 'Wi-Fi', 'CalDAV', and 'CardDAV'. The main content area is titled 'Wi-Fi' and includes fields for 'Netzwerkname (SSID)', 'Sicherheitstyp' (set to WPA/WPA2), and 'Kennwort'. There are also checkboxes for 'Unsichtbares Netzwerk' and 'Netzwerkname (SSID)'. At the top right of the main content area, there are minus and plus signs for managing the list of networks.





## iOS Enterprise Funktionen



**VPN:**

Es können mehrere VPNs konfiguriert werden.

Man beachte das – und +

**VPN**

**Verbindungsname**  
Angezeigter Name der Verbindung (auf dem Gerät)  
[erforderlich]

**Verbindungstyp**  
Der Verbindungstyp, der durch diese Vorgabe aktiviert wird

- L2TP
- PPTP
- Phase 1/2 Cisco
- Cisco AnyConnect
- Juniper SSL

**Account**  
Benutzeraccount für die Authentifizierung der Verbindung  
[auf Gerät festlegen]

**Benutzerauthentifizierung**  
Authentifizierungstyp für die Verbindung  
 Kennwort  RSA-SecurID

**Schlüssel (Shared Secret)**  
Schlüssel (Shared Secret) für die Verbindung  
[optional]

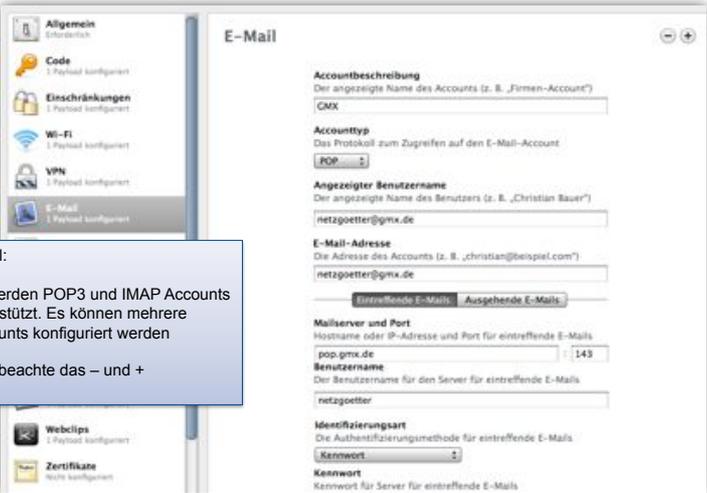
**Für alle Daten**  
Leitet gesamten Netzwerkverkehr über die VPN-Verbindung

**Proxy-Konfiguration**  
Proxies für diese VPN-Verbindung konfigurieren.  
[Ohne]





## iOS Enterprise Funktionen



**E-Mail:**

Es werden POP3 und IMAP Accounts unterstützt. Es können mehrere Accounts konfiguriert werden

Man beachte das – und +

**E-Mail**

**Accountbeschreibung**  
Der angezeigte Name des Accounts (z. B. „Firmen-Account“)  
GMX

**Accounttyp**  
Das Protokoll zum Zugriff auf den E-Mail-Account  
POP

**Angezeigter Benutzername**  
Der angezeigte Name des Benutzers (z. B. „Christian Bauer“)  
netzgoetter@gmx.de

**E-Mail-Adresse**  
Die Adresse des Accounts (z. B. „christian@beispiel.com“)  
netzgoetter@gmx.de

Eintreffende E-Mails  Ausgehende E-Mails

**Mailserver und Port**  
Hostname oder IP-Adresse und Port für eintreffende E-Mails  
pop.gmx.de 143

**Benutzername**  
Der Benutzername für den Server für eintreffende E-Mails  
netzgoetter

**Identifizierungsart**  
Die Authentifizierungsmethode für eintreffende E-Mails  
Kennwort

**Kennwort**  
Kennwort für Server für eintreffende E-Mails

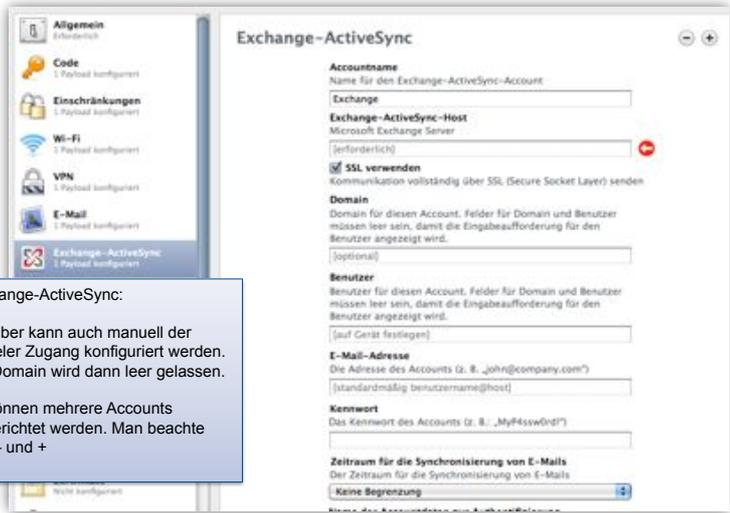


iOS Enterprise Funktionen


**Exchange-ActiveSync:**

Hierüber kann auch manuell der Traveler Zugang konfiguriert werden. Die Domain wird dann leer gelassen.

Es können mehrere Accounts eingerichtet werden. Man beachte das – und +



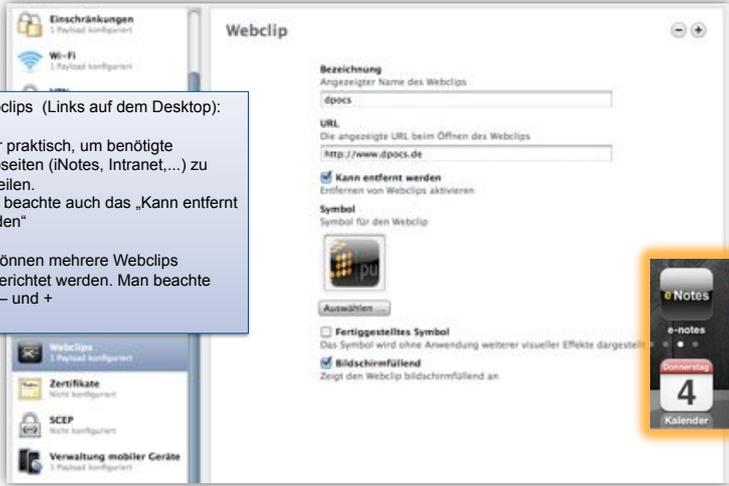

31

iOS Enterprise Funktionen


**Webclips (Links auf dem Desktop):**

Sehr praktisch, um benötigte Webseiten (iNotes, Intranet,...) zu Verteilen. Man beachte auch das „Kann entfernt werden“

Es können mehrere Webclips eingerichtet werden. Man beachte das – und +




32

### iOS Enterprise Funktionen



**Zertifikate:**  
Alle auf dem Gerät benötigten Zertifikate können hierüber verteilt werden.  
VPN, Root-Zertifikate, CodeSigner Zertifikate

**Zertifikate konfigurieren**  
Hier können Sie die PKCS1- und PKCS12-Zertifikate festlegen, die auf dem Gerät installiert werden sollen. Fügen Sie Ihr Firmenzertifikat hinzu sowie weitere Zertifikate, die für das Verbinden des Geräts mit dem Netzwerk erforderlich sind.

**Konfigurieren**



### iOS Enterprise Funktionen



**Allgemein** Erforderlich

**Code** 1 Payload konfiguriert

**Einschränkungen** 1 Payload konfiguriert

**Wi-Fi** 1 Payload konfiguriert

**E-Mail** 1 Payload konfiguriert

**Exchange-ActiveSync** 1 Payload konfiguriert

**Abonnierte Kalender** 1 Payload konfiguriert

**Webclips** 1 Payload konfiguriert

**Profil installieren**

**AdminCamp 2010**

**Überprüfen**

**Profilbeschreibung:**  
iPhone Configuration Utility  
89F40D0D-99C0-418A-A40E-8E46C1040000

**Erhalten:** 17.08.2010

**Erweitert:**  
Web-Clip  
Wi-Fi-Netzwerk  
Kalenderabonnement  
Exchange Account  
E-Mail Account  
LDAP Account  
Namenverzeichnis

**Mehr Details**



### iOS Enterprise Funktionen



- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert



### iOS Enterprise Funktionen



- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert



### iOS Enterprise Funktionen



- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert



### iOS Enterprise Funktionen



- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert



## iOS Enterprise Funktionen

- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert

39

## iOS Enterprise Funktionen

**Profilsicherheit:**

**Immer** = User kann Profil manuell entfernen

**Mit Autorisierung** = Profil kann nur nach Eingabe eines Kennwortes entfernt werden

**Nie** = Profil kann nicht gelöscht werden. Hier hilft nur ein Reset des Geräts

Wird das Profil gelöscht,

werden alle über das Profil erstellten Payloads inkl. der dazugehörigen Daten entfernt.

Traveler oder IMAP Payloads die Mails, WLAN Payloads, die WLAN Konfig.

Praktisch oder?

40

**iOS Enterprise Funktionen**



- Allgemein**  
Erforderlich
- Code**  
1 Payload konfiguriert
- Einschränkungen**  
1 Payload konfiguriert
- Wi-Fi**  
1 Payload konfiguriert
- E-Mail**  
1 Payload konfiguriert
- Exchange-ActiveSync**  
1 Payload konfiguriert
- Abonnierte Kalender**  
1 Payload konfiguriert
- Webclips**  
1 Payload konfiguriert



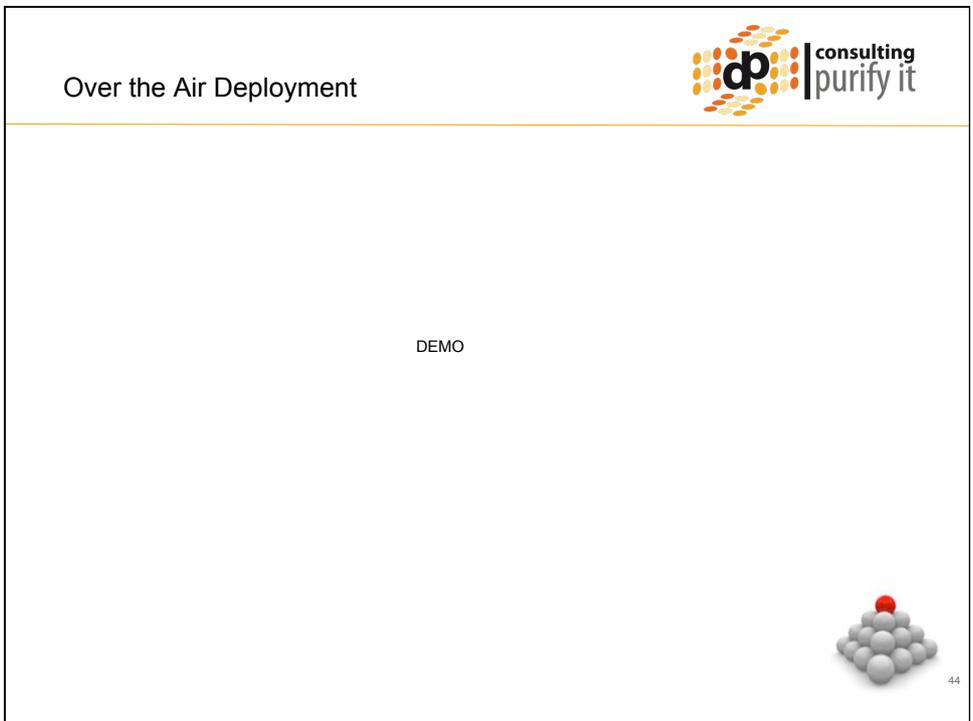
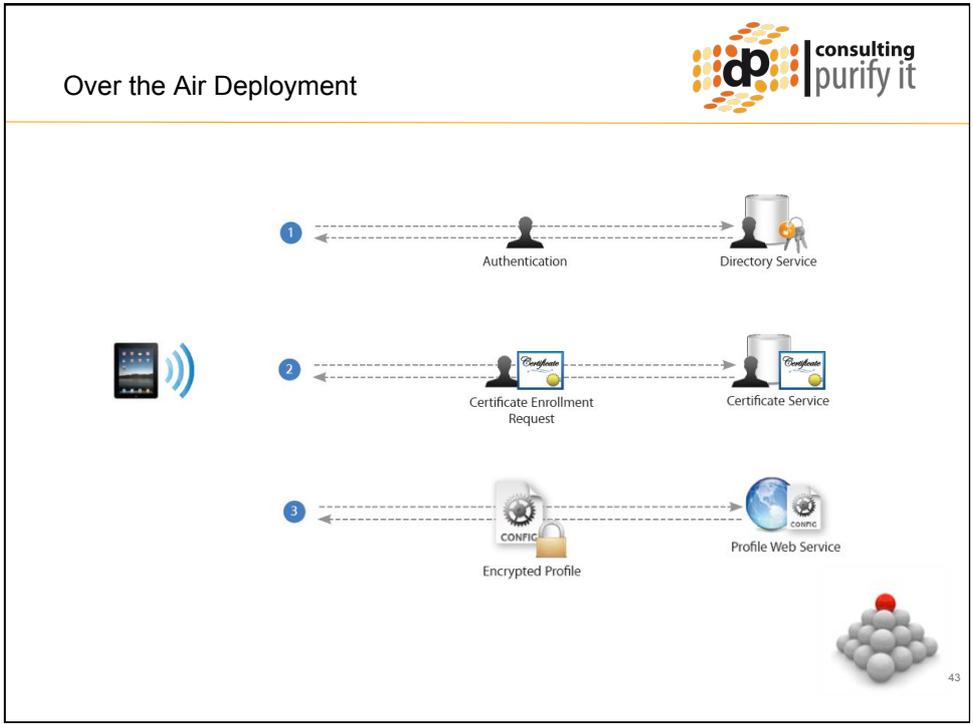
Configuration Profiles

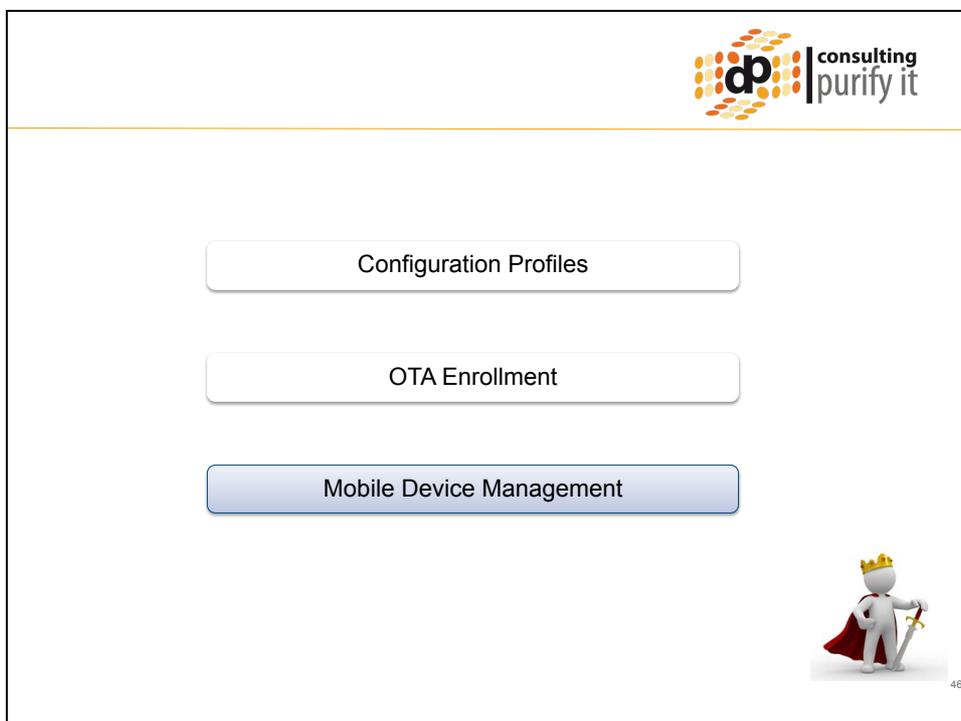
OTA Enrollment

Mobile Device Management



42





Mobile Device Management


---

Device Management ermöglicht:

- Transparent Verwaltung über WLAN oder GPRS
- Kommunikation per HTTPS
  
- Features:
  - Remote Commands
    - Install / Remove Profiles
    - Lock / Erase Devices
    - Passcode zurücksetzen
  
  - Queries
    - Netzwerkinformationen (Data Roaming, Carrier,...)
    - Device-Informationen (Model, OS, Firmware, IMEI,...)
    - App-Informationen (inst. Apps & Profiles)
    - Compliance / Security Informationen



47

Mobil Device Management


---

How does it Work?

1. OTA Enrollment

3. Install MDM Profil

4. Binden MDM Srv

2. Erzeuge MDM Profile



MDM Server





Initiale Einrichtung



Notification Service



48

Mobile Device Management



DEMO



9

Mobil Device Management



How does it Work?

1. Sende MDM Push      2. Nachricht an Device      3. Verbindung zu MDM



4. Befehle & Abfragen per Profile-Payload

Aktives Management



50

Mobile Device Management



DEMO



1

The Missing Link



Fazit:

iOS Geräte sind aus meiner Sicht Enterprise-fähig und können in fast allen Bereichen die Anforderungen mehr als Abdecken.

Mit Traveler ist eine nahtlose Integration ohne Mehrkosten in eine Domino Infrastruktur vorhanden.

Mit OTA & MDM stehen alle Mittel zur Verfügung, um zentral iPhone/iPads automatisiert zu konfigurieren und Sicherheitsstandards zu erzwingen.

Es ist aber nicht mit einer Traveler Einrichtung getan!



52



Informationen:

<http://www.apple.com/iphone/business/integration/>

**Deployment Resources**

**Enterprise Deployment Scenarios**  
Learn how iPhone integrates seamlessly into enterprise environments with these deployment scenarios and device configuration overviews.

- All deployment scenarios
- Microsoft Exchange ActiveSync
- Standards-Based Services
- Virtual Private Networks (VPN)
- Wi-Fi
- Digital Certificates
- Mobile Device Management
- iTunes Deployment

**Enterprise Deployment Guide**  
The comprehensive guide for system administrators on how to integrate iPhone with enterprise systems.

[Access the deployment guide](#)

**iPhone Configuration Utility**  
A desktop application for IT administrators to easily create, maintain, and sign configuration profiles.

[Download the application](#)



Informationen:

1-tägiger Workshop:

Lotus Traveler & iOS Devices

- Lotus Traveler Konzept, Infrastruktur & Sicherheit
- Sicheres & automatisiertes Deployment von iOS Devices

Veranstaltet von Daniel Nashed & Detlev Pöttgen

Ort & Termine in Kürze oder auf Anfrage bei Ihnen Inhouse



That's it .... Vielen Dank



Mein Blog  
(Präsentation + Links):

<http://www.netzgoetter.net>

