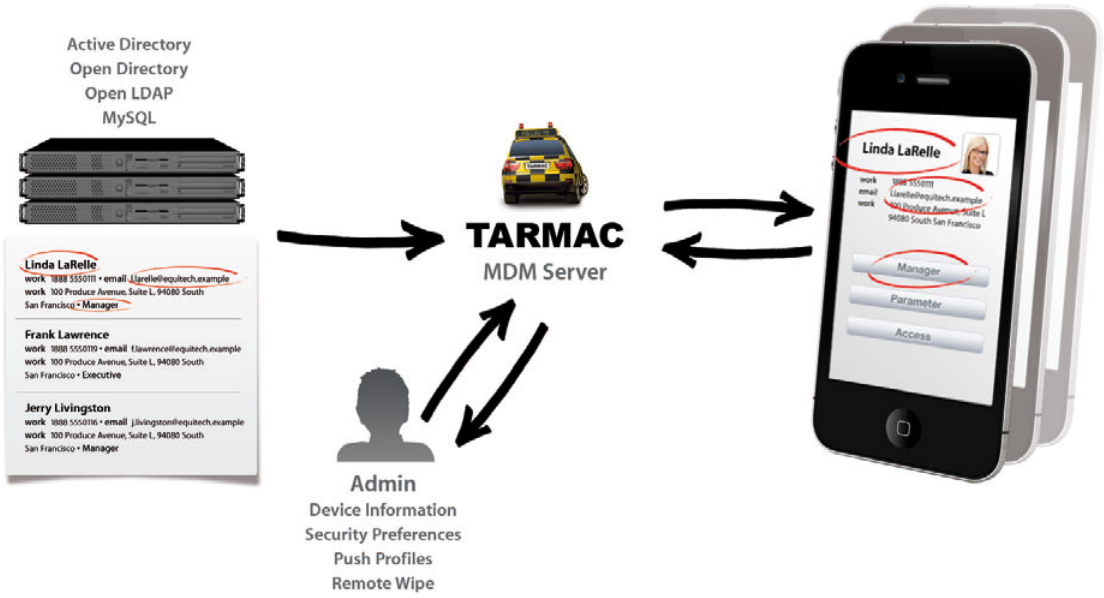
e·quinux

TARMAC

iPhones & iPads unternehmensweit integrieren

TARMAC arbeitet als Middleware zwischen Verzeichnisdiensten und den iPhones und iPads Ihrer Mitarbeiter und integriert Apples Mobilgeräte sicher und zuverlässig in die Unternehmens-IT. Die intuitive Oberfläche und der effiziente Workflow sparen Ihnen, Ihren IT-Verantwortlichen und Ihren Mitarbeitern Kosten und Zeit.



TARMAC und seine Funktionen

Mobilgeräte over-the-air (OTA) einrichten
Verteilen Sie iPhones und iPads unternehmensweit ohne diese lokal mit einem Rechner verbinden zu müssen.

Benutzerprofile entfernt installieren
TARMAC erzeugt automatisch personalisierte Profile, in denen Einstellungen, Zugriffsdaten und Geräte-vorgaben festgelegt sind.

Mehr Sicherheit mit Mobile Device Management
Mit Mobile Device Management verwalten Sie Mobilgeräte noch zuverlässiger und profitieren von erweiterten Steuerungsmöglichkeiten.

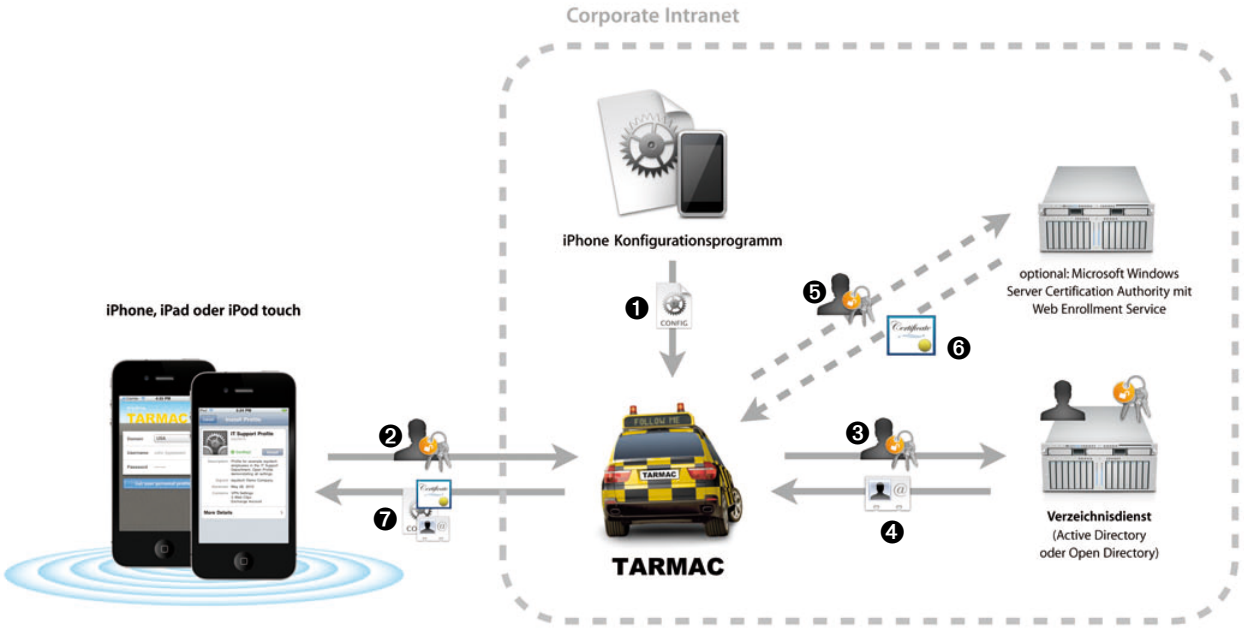
Mit Inventory Management Kosten sparen
TARMAC verwaltet installierte Benutzerprofile der Anwender zentral. Und reduziert Kosten von der Integration bis zur Verwaltung der Mobilgeräte.

Apple Mobilgeräte sicher integrieren
Das ausgeklügelte Zertifikate-Management garantiert die Integrität Ihrer Daten bei der Provisionierung und der Administration.

Alle Aktionen sicher durchführen
Mit TARMAC verlassen keine Daten die interne Infrastruktur. Durch die zentrale Provisionierung lassen sich sicherheitsrelevante Änderungen sofort umsetzen.

Überblick über Daten und Profile behalten
Da TARMAC ohne Client-Software auf dem Endgerät auskommt, behalten Sie jederzeit die Kontrolle über Ihre Daten.

Dank Skalierbarkeit nachhaltig investieren
TARMAC ist aufwärts skalierbar. Der Administrator legt neue Nutzer zentral im Verzeichnisdienst an. Diese können sofort von TARMAC profitieren.



TARMAC Konfiguration von iPad und iPhone

❶ Konfiguration initial festlegen – TARMAC befüllt die Konfigurationsvorlage des Administrators automatisch mit allen Daten aus dem Verzeichnisdienst.

❷ Anmeldung des Benutzers sowie seines Endgerätes an der TARMAC Webschnittstelle – entweder direkt aus dem internen Netzwerk oder auf Wunsch HTTPS verschlüsselt über das Internet.

❸ TARMAC wählt die vom Administrator zugewiesene Konfiguration.

❹ Der Verzeichnisdienst liefert die Daten für diesen Benutzer.

❺ TARMAC verfügt über SCEP (Simple Zertifikate Enrollment Protocol) mit integriertem Zertifikateserver (CA = Certificate Authority).

❻ Optional hinterlegt der Administrator ein eigenes Zertifikat beim integrierten Zertifikateserver oder fordert von der Microsoft Windows Server Certification Authority ein Microsoft Exchange Zertifikat an.

❼ TARMAC generiert ein vollständig personalisiertes Konfigurationsprofil für den Benutzer – inklusive Exchange Anmeldedaten aus dem Active Directory und aller festgelegten Restriktionen.

TARMAC im Detail

Egal, ob Administratoren Profile für Firmengeräte bereitstellen möchten oder Endnutzer ihr privates iPhone oder iPad für Unternehmenszwecke einrichten wollen, TARMAC unterstützt beide Szenarien.

Administration von Profilen

Die Verwaltung von Profilen ist mit TARMAC einfach: Der Administrator erstellt Profile mit dynamischen Parametern und trägt spezielle Platzhalter-Notationen ein. Diese Platzhalter füllt TARMAC automatisch mit dem Inhalt des entsprechenden Verzeichnisdienst-Attributs für den aktuellen Benutzer. Der Zugriff auf Profile lässt sich gruppenbasierend einschränken. Das Ergebnis? Profile werden effizient und sicher über das Internet verteilt (OTA).

Sicher mit TARMAC

Auch beim Einrichten bleiben Anwender mit TARMAC auf der sicheren Seite: Um eine direkte Verbindung zur TARMAC Weboberfläche herzustellen, müssen auf dem TARMAC Server nur die unbedingt benötigten Ports geöffnet werden: HTTP (80) oder HTTPS (443). Generell greifen Anwender abgeschottet im eigenen Firmen-Intranet (WLAN) auf TARMAC zu.

Auf Wunsch kann der Zugriff auch über ein mobiles Datennetzwerk erfolgen (UMTS). In diesem Fall muss der TARMAC Server aus dem Internet (beispielsweise über Reverse Proxy) erreichbar sein.

Datenschutz im Blick – auch in Sachen Speicherung. Außer den definierten Konfigurationsprofilen speichert der TARMAC Server keine Zugangsdaten. Diese werden beim bestehenden zentralen Verzeichnisdienst abgefragt.

TARMAC in der IT-Infrastruktur
TARMAC lässt sich einfach konfigurieren. Dazu sind lediglich die Verbindungsparameter zum Open Directory oder Active Directory, das über LDAP angesprochen wird, nötig.

Für Abfragen des LDAP-Servers wird ein hinterlegter technischer Account verwendet oder ohne Account Daten (Anonymous Bind) zugegriffen. In beiden Fällen sind lediglich Leserechte nötig, um die zum angemeldeten Benutzer passenden Attribute zu ermitteln.

Ist die initiale Konfiguration abgeschlossen, verlangt TARMAC zum Verwalten von Konfigurationsprofilen und Anwendern nach einem gültigen Verzeichnisdienst-Benutzer aus einer der Administratoren-Gruppen.

Microsoft CA in TARMAC
Keine Kompromisse in Sachen Sicherheit – TARMAC kann direkt mit einer Microsoft Windows Server Certification Authority mit Web Enrollment Service zusammenarbeiten. Über die Web Enrollment Service URL der Microsoft CA fragt TARMAC die Zertifikate für die Exchange Authentifizierung ab und integriert sie direkt in die Konfigurationsprofile.

Adminstratoren können auch die integrierte Certificate Authority (CA) von TARMAC verwenden und dort eigene Zertifikate hinterlegen, um vertrauliche Daten beim Übermitteln zu verschlüsseln. Und wieder zu entschlüsseln. Denn TARMAC erlaubt den Roll-Out über SCEP (Simple Certificate Enrollment Protocol).

Protokollierung in TARMAC
TARMAC zeigt übersichtlich, welcher Benutzer bereits ein Profil installiert hat. Und protokolliert einzelne Zugriffsversuche sowie Datum, Benutzername, Profilname und Zugriffe. So lassen sich Probleme proaktiv im entsprechenden Kontext lösen.

Apps unternehmensweit bereitstellen mit TARMAC
Firmeninterne Apps (AdHoc oder Inhouse) können durch TARMAC für Benutzer via Wi-Fi leicht zugänglich gemacht werden. Dazu hinterlegt der Administrator die Apps beispielsweise auf einem HTTPS-Server.

Per Klick aktivieren die User die App und installieren sie auf ihren Apple Mobilgeräten – drahtlos und ohne eine Verbindung zu ihrem Computer herstellen zu müssen.

Mobile Device Management. Erreichen Sie den nächsten Sicherheitslevel.

Die Zentrale für Konfiguration, Rollout und Verwaltung von iPad & iPhone
Mit Mobile Device Management (MDM) unterstützt TARMAC alle Befehle, die iOS4 auf dem iPad oder iPhone zum Verwalten und Managen der Geräte over-the-air erlaubt.

Automatische Konfiguration von Anwendungen, Diensten und Funktionen
TARMAC kommuniziert nach der Anmeldung mit dem iPhone oder iPad, so dass der Administrator alle Aktionen automatisch und unternehmensweit durchführen kann.

Individuelle Profile erstellen und Benutzerprofile aktualisieren
In den Profilen legt der Administrator individuelle Einstellungen fest. Diese kann er – ohne Zutun des Anwenders – je nach Unternehmenserfordernissen im Hintergrund updaten und aufspielen.

Updates und Einstellungen ändern – per Push
Sicherheits-Updates oder Profiländerungen werden per Push-Funktion auf iPad oder iPhone gebracht und im Hintergrund installiert.

Passwörter over-the-air zurücksetzen
Zugangsdaten vergessen? Kein Problem. Der Administrator setzt das Passwort over-the-air zurück – ohne das Gerät völlig neu konfigurieren zu müssen.

iPhone oder iPad remote löschen
Der Administrator kann ein liegen gebliebenes Gerät sperren, das Passwort zurücksetzen oder die Daten komplett löschen – over-the-air.

Ihre Vorteile im Überblick

- Profitieren Sie von maximaler Sicherheit dank Mobile Device Management
- Stellen Sie Apps unternehmensweit zur Verfügung
- Verteilen und aktualisieren Sie Profile noch schneller
- Freuen Sie sich über weniger Support-Anfragen
- Setzen Sie Ihre Sicherheitsrichtlinien unternehmensweit um
- Entlasten Sie Ihre Mitarbeiter durch automatische Profilupdates
- Behalten Sie die Kontrolle über Ihre IT
- Überblicken Sie Ihr Inventory Management

Referenzkunden

sanofi aventis
Das Wichtigste ist die Gesundheit

TECHNISCHE UNIVERSITÄT MÜNCHEN

Händlerstempel

Weitere Informationen

Sie haben Fragen oder möchten sich detailliert über TARMAC Mobile Device Management informieren? Kontaktieren Sie unsere TARMAC Experten per Mail unter **TARMAC@equinux.com**.

Systemvoraussetzungen für TARMAC Server

- Intel Mac mit Mac OS X 10.5, 10.6
- oder: Intel Mac mit Mac OS X Server 10.5, 10.6

Systemvoraussetzungen für die TARMAC Administration

- jeder Webbrowser der CSS 3 unterstützt, z.B. Internet Explorer 8, Firefox 3, Safari, Google Chrome

Unterstützte Verzeichnisdienste

- Mac OS X Server 10.5 (Leopard) mit Open Directory
- Mac OS X Server 10.6 (Snow Leopard) mit Open Directory
- Microsoft Windows Server 2008 mit Active Directory Domain Services (ADDS)
- Microsoft Windows Server 2003 mit Active Directory (AD)
- jeder MySQL Server

Unterstützte Zertifikat-basierende Exchange Authentifizierung

- Microsoft Windows Server 2003 Certification Authority mit Web Enrollment Service
- Microsoft Windows Server 2008 Certification Authority mit Web Enrollment Service

Unterstützte E-Mail Dienste

- Microsoft Exchange Server 2003 mit Exchange ActiveSync (EAS)
- Microsoft Exchange Server 2007 mit Exchange ActiveSync (EAS)
- jeder IMAP4 E-Mail Server
- jeder POP3 E-Mail Server

Unterstützte Kalender Dienste

- Microsoft Exchange Server 2003 mit Exchange ActiveSync (EAS)
- Microsoft Exchange Server 2007 mit Exchange ActiveSync (EAS)
- Mac OS X Server 10.6 (Snow Leopard) mit iCal Server
- CalDAV kompatible Server

Unterstützte Adressbücher

- Microsoft Exchange Server 2003 mit Globalem Adressbuch (GAL)
- Microsoft Exchange Server 2007 mit Globalem Adressbuch (GAL)
- LDAPv3-Server kompatible Server

Headquarter
equinux AG
Informationstechnologien
Kirschstr. 35
80999 München
Tel. (089) 520 465 - 222
Fax (089) 520 465 - 299

US-Niederlassung
equinux USA, Inc.
100 Produce Ave., Suite L
South San Francisco
CA 94080, USA
Tel. (650) 200 4589 Ext. 222
Fax (650) 200 872 1907