iPhone OS
Einsatz in Unternehmen

Zweite Auflage, für Version 3.2 oder neuer

Apple
1 Infinite Loop
Cupertino, CA 95014
408-996-1010
www.apple.com

D019-1835 / April 2010

Inhalt

Das iPhone in Unternehmen

Das vorliegende Dokument beschreibt die Integration von iPhone, iPod touch und iPad in Unternehmen.

Dieses Handbuch ist für Systemadministratoren konzipiert und umfasst Informationen zur Implementierung und Unterstützung von iPhone und iPod touch und iPad in Unternehmensumgebungen.

Neuerungen für Unternehmen in iPhone OS 3.0 und neuer

iPhone OS 3.x bietet eine Vielzahl von Erweiterungen und Verbesserungen, die besonders für Unternehmenskunden und deren Benutzer interessant sind:

- Unterstützung für die drahtlose Synchronisierung von CalDAV-Kalendern
- LDAP-Serverunterstützung für die Suche nach Kontakten zur Verwendung in E-Mails, Adressbüchern und SMS-Nachrichten
- Verschlüsseln von Konfigurationsprofilen und administrative Kennwörter als Schutz vor dem Löschen der Profile vom Gerät
- iPhone-Konfigurationsprogramm zum direkten Hinzufügen und Entfernen verschlüsselter Konfigurationsprofile auf über USB angeschlossenen Geräten
- Unterstützung für OCSP (Online Certificate Status Protocol) für den Rückruf von Zertifikaten
- Unterstützung für zertifikatbasierte VPN-On-demand-Verbindungen
- Unterstützung für VPN-Proxy-Konfiguration mittels Konfigurationsprofil und VPN-Server
- Möglichkeit für Microsoft Exchange-Benutzer, andere Benutzer zu Meetings einzuladen, Möglichkeit für Benutzer von Microsoft Exchange 2007, den Antwortstatus anzuzeigen
- Unterstützung für die zertifikatbasierte Identifizierung mithilfe eines Exchange ActiveSync-Clients
- Unterstützung für zusätzliche EAS-Richtlinien und für das EAS-Protokoll 12.1

- Zusätzliche Einschränkungen für Geräte (u. a. Festlegen der Kulanzzeit, während der das Gerät entsperrt bleibt, Deaktivieren der Kamera und Verhindern, dass Benutzer ein Bildschirmfoto der Anzeige des Geräts erstellen)
- Durchsuchen lokal gespeicherter E-Mail-Nachrichten und Kalenderereignisse Möglichkeit zum Durchsuchen auf einem IMAP-, MobileMe- oder Exchange 2007-Server gespeicherter E-Mails
- Einbeziehung weiterer Mail-Ordner in die Zustellung per Push-Funktion
- Möglichkeit zur Festlegung der APN-Proxy-Einstellungen in einem Konfigurationsprofil
- Möglichkeit zur Installation von Web-Clips mithilfe eines Konfigurationsprofils
- Unterstützung für 802.1x EAP-SIM
- Drahtlose Identifizierung und Registrierung von Geräten mithilfe eines SCEP-Servers (Simple Certificate Enrollment Protocol)
- Möglichkeit zum Speichern verschlüsselter Gerätedatensicherungen in iTunes
- Unterstützung für Profilerstellung über Skripts im iPhone-Konfigurationsprogramm
- Unterstützung von iPad, iPhone und iPod touch im iPhone-Konfigurationsprogramm 2.2. Mac OS X 10.6 Snow Leopard ist erforderlich. Windows 7 wird ebenfalls unterstützt.

Systemanforderungen

Hier finden Sie einen Überblick über die Systemanforderungen und über die Komponenten, die für die Integration von iPhone, iPod touch und iPad in Unternehmenssysteme zur Verfügung stehen.

iPhone und iPod touch

Die im Netzwerk Ihres Unternehmens verwendeten iPhone- und iPod touch-Geräte müssen mit iPhone OS 3.1.x aktualisiert werden.

iPad

Das iPad muss mit iPhone OS 3.2.x aktualisiert werden.

iTunes

Für die Konfiguration der Geräte ist iTunes 9.1 (oder neuer) erforderlich. iTunes wird auch für das Installieren von Softwareaktualisierungen für iPhone, iPod touch und iPad benötigt. Ferner verwenden Sie iTunes auch für das Installieren von Programmen und für das Synchronisieren von Musik, Videos, Notizen und anderen Daten mit einem Mac oder PC.

Damit Sie iTunes verwenden können, benötigen Sie einen Mac-Computer oder einen PC mit einem USB 2.0-Port, der den Mindestanforderungen genügt, die auf der folgenden Website aufgeführt sind: www.apple.com/de/itunes/download/.

iPhone-Konfigurationsprogramm

Mit dem iPhone-Konfigurationsprogramm können Sie Konfigurationsprofile erstellen, verschlüsseln und installieren, Vorlageprofile und autorisierte Programme überwachen und installieren sowie Konsolenprotokolle und andere gerätespezifische Informationen erfassen.

Für das iPhone-Konfigurationsprogramm ist eines der folgenden Betriebssysteme erforderlich:

- Mac OS X 10.5 Snow Leopard
- Windows XP Service Pack 3 mit .NET Framework 3.5 Service Pack 1
- Windows Vista Service Pack 1 mit .NET Framework 3.5 Service Pack 1
- Windows 7 mit .NET Framework 3.5 Service Pack 1

Das iPhone-Konfigurationsprogramm kann unter den 32- und den 64-Bit-Versionen der Windows-Betriebssysteme ausgeführt werden.

Das .Net Framework 3.5 Service Pack 1-Installationsprogramm kann unter folgender Adresse geladen werden:
http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

Das Programm bietet die Möglichkeit, eine Outlook-Nachricht mit einem Konfigurationsprofil als Anhang zu erstellen. Darüber hinaus können die Namen und E-Mail-Adressen von Benutzern aus dem Adressbuch des Desktop-Computers auf Geräte übertragen werden, die an den Computer angeschlossen und mit dem Programm verbunden sind. Für beide genannten Funktionen ist das Programm „Outlook“ erforderlich. Sie sind nicht mit dem Programm „Outlook Express“ kompatibel. Damit Ihnen diese Funktionen auf einem Computer unter Windows XP zur Verfügung stehen, müssen Sie möglicherweise die Update-Software „2007 Microsoft Office System Update: Redistributable Primary Interop Assemblies“ installieren. Die Installation dieser Software ist erforderlich, wenn das Programm „Outlook“ vor dem .NET Framework 3.5 Service Pack 1 installiert wurde.

Das Primary Interop Assemblies-Installationsprogramm ist verfügbar unter:
http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

iPhone, iPod touch und iPad unterstützen die folgenden Microsoft Exchange-Versionen:

- Exchange ActiveSync für Exchange Server (EAS) 2003 Service Pack 2
- Exchange ActiveSync für Exchange Server (EAS) 2007

Damit die Richtlinien und Funktionen von Exchange 2007 unterstützt werden, ist das Service Pack 1 erforderlich.

Unterstützte Exchange ActiveSync-Richtlinien (Policies)

Die folgenden Exchange-Richtlinien werden unterstützt:

- Zwingende Eingabe eines Gerätekennworts
- Mindestlänge für Kennwort
- Maximale Anzahl von Fehlversuchen bei der Code-Eingabe
- Kennwort muss aus Ziffern und Buchstaben bestehen
- Inaktivitätszeit in Minuten

Die folgenden Exchange 2007-Richtlinien werden ebenfalls unterstützt:

- Zulassen bzw. Zurückweisen einfacher Kennwörter
- Verfallszeit für Kennwörter
- Kennwortchronik
- Intervall für Aktualisierung von Richtlinien
- Mindestanzahl komplexer Zeichen in Kennwörtern
- Notwendigkeit zum manuellen Synchronisieren beim Roaming
- Aktivieren der Kamera
- Notwendigkeit der Geräteverschlüsselung

Eine Beschreibung der einzelnen Richtlinien finden Sie in der Dokumentation zu Exchange ActiveSync.

Die Exchange-Richtlinie für die Geräteverschlüsselung (RequireDeviceEncryption) wird vom iPhone 3GS, iPod touch (Mod. Herbst 2009 mit 32 GB oder mehr) und iPad unterstützt. iPhone, iPhone 3G und andere iPod touch-Modelle unterstützen die Geräteverschlüsselung nicht und stellen keine Verbindung zu einem Exchange Server her, der diese Funktion voraussetzt.

Wenn Sie die Richtlinie „Erfordert Zahlen und Buchstaben“ (Exchange 2003) bzw. „Alphanumerisches Kennwort erforderlich“ (Exchange 2007) aktivieren, muss der Benutzer einen Gerätecode eingeben, der mindestens ein komplexes Zeichen enthält.

Mit dem Wert, der durch die Richtlinie für die Inaktivitätszeit (MaxInactivityTimeDeviceLock oder AEFrequencyValue) angegeben wird, wird der Maximalwert festgelegt, den Benutzer unter „Einstellungen“ > „Allgemein“ > „Automatische Sperre“ und „Einstellungen“ > „Allgemein“ > „Code-Sperre“ > „Code anfordern“ auswählen können.

Fernlöschen

Der Inhalt eines iPhone, iPod touch oder iPad kann per Fernzugriff gelöscht werden (Fernlöschen). Auf diese Weise lassen sich alle Daten und Konfigurationsinformationen vom Gerät entfernen. Nach dem sicheren Löschen des Geräts werden die ursprünglichen Werkseinstellungen wiederhergestellt.

Wichtig: Auf dem iPhone und iPhone 3G werden die Daten auf dem Gerät beim Löschen überschrieben. Der Löschvorgang dauert pro 8 GB Speicherkapazität ungefähr eine Stunde. Das Gerät sollte daher vor Beginn des Löschvorgangs an eine Stromquelle angeschlossen werden. Schaltet sich das Gerät während des Löschvorgangs aufgrund einer zu schwachen Batterie ab, wird der Vorgang fortgesetzt, sobald das Gerät mit Strom versorgt wird. Auf dem iPhone 3GS und iPad wird der Verschlüsselungscode für die Daten (die mit 256-Bit-AES-Verschlüsselung verschlüsselt sind) beim Löschen entfernt. Der Löschvorgang erfolgt dabei sofort.

Unter Exchange Server 2007 kann das Fernlöschen über die Exchange-Verwaltungskonsole, Outlook Web Access oder das Exchange ActiveSync Mobile Administration Web Tool gestartet werden.

Unter Exchange Server 2003 kann das Fernlöschen über das Exchange ActiveSync Mobile Administration Web Tool gestartet werden.

Die Benutzer haben darüber hinaus die Möglichkeit, ein in ihrem Besitz befindliches Gerät mithilfe der Option „Inhalte & Einstellungen löschen" im Menü „Zurücksetzen" des Bereichs „Allgemein" zu löschen. Die Geräte lassen sich auch so konfigurieren, dass nach mehreren fehlgeschlagenen Anmeldeversuchen (durch Eingabe des falschen Codes) das Gerät automatisch vollständig gelöscht wird.

Wenn Sie ein Gerät wiederherstellen, dessen Daten gelöscht wurden, weil es verloren ging, stellen Sie die Daten mithilfe von iTunes und der neusten Sicherungskopie des Geräts wieder her.

Microsoft Direct Push

iPhone und iPad Wi-Fi + 3G werden vom Exchange-Server automatisch mit E-Mails, Kontaktinformationen und Kalendereintragungen beliefert, solange eine Mobilfunk- oder eine Wi-Fi-Datenverbindung besteht. iPod touch und iPad Wi-Fi, die keine Mobilfunkverbindung besitzen, werden im Gegensatz dazu nur mit Push-Informationen versorgt, solange die Geräte aktiv und mit einem Wi-Fi-Netzwerk verbunden sind.

Microsoft Exchange Autodiscovery-Funktion

Der Autodiscover-Dienst von Exchange Server 2007 wird unterstützt. Wenn Sie ein Gerät manuell konfigurieren, verwendet der Autodiscover-Dienst Ihre E-Mail-Adresse und Ihr Kennwort, um automatisch die richtigen Exchange-Server-Informationen zu ermitteln. Informationen über das Aktivieren des Autodiscover-Diensts finden Sie im Internet unter der folgenden Adresse: http://technet.microsoft.com/en-us/library/cc539114.aspx.

Microsoft Exchange Globale Adressliste (GAL)

iPhone, iPod touch und iPad rufen die Kontaktinformationen aus dem unternehmensspezifischen Verzeichnis (Corporate Directory) des Exchange-Servers ab. Sie können auf dieses Verzeichnis zugreifen, wenn Sie in den Kontakten suchen. Beim Eingeben von E-Mail-Adressen wird ebenfalls auf das Verzeichnis zugegriffen, um Ihre Eingaben automatisch zu vervollständigen.

Zusätzlich unterstützte Exchange ActiveSync-Funktionen

Zusätzlich zu den bereits beschriebenen Funktionen und Leistungsmerkmalen unterstützt das iPhone OS folgende Optionen:

- Erstellen von Einladungen mithilfe des Kalenders. Benutzer von Microsoft Exchange 2007 haben zusätzlich die Möglichkeit, den Status der Antworten auf ihre Einladungen anzuzeigen.
- Kennzeichnen von Kalenderereignissen als „Frei“, „Belegt“, „Provisorisch“ oder „Nicht anwesend“
- Durchsuchen auf dem Server gespeicherter E-Mails. Hierfür ist Microsoft Exchange 2007 erforderlich.
- Zertifikatbasierte Identifizierung mithilfe eines Exchange ActiveSync-Clients

Nicht unterstützte Exchange ActiveSync-Funktionen

Zu den nicht unterstützten Exchange-Funktionen gehören unter anderem:

- Ordnerverwaltung
- Öffnen von Links in E-Mails, die auf Dokumente verweisen, die auf Sharepoint-Servern gespeichert sind
- Synchronisieren von Aufgaben
- Festlegen einer automatischen Abwesenheitsnotiz
- Markieren von Nachrichten zur Nachverfolgung

VPN

iPhone OS kann mit VPN-Servern verwendet werden, die folgende Protokolle und Identifizierungsverfahren unterstützen:

- L2TP/IPSec mit Benutzeridentifizierung durch MS-CHAPV2-Kennwort, RSA SecurID und CryptoCard sowie Geräteidentifizierung durch Shared Secret (symmetrischer Schlüssel).
- PPTP mit Benutzeridentifizierung durch MS-CHAPV2-Kennwort, RSA SecurID und CryptoCard.
- Cisco IPSec mit Benutzeridentifizierung durch Kennwort, RSA SecurID oder CryptoCard sowie Geräteidentifizierung durch Shared Secret und Zertifikate. In Anhang A finden Sie kompatible Cisco-VPN-Server sowie Konfigurationsempfehlungen.

Cisco IPSec mit zertifikatbasierter Identifizierung unterstützt VPN on Demand für die Domänen, die bei der Konfiguration definiert werden. Weitere Informationen finden Sie im Abschnitt „Einstellungen im Bereich „VPN““ auf Seite 40.

Netzwerksicherheit

iPhone OS unterstützt die folgenden, von der Wi-Fi-Allianz definierten 802.11i-Sicherheitsprotokolle für drahtlose Netzwerke:

- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

Darüber hinaus unterstützt das iPhone OS die folgenden 802.1X-Identifizierungsverfahren für WPA Enterprise- und WPA2 Enterprise-Netzwerke:

- EAP-TLS
- EAP -TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, PEAP v1
- LEAP

Zertifikate und Identitäten

iPhone, iPod touch und iPad unterstützen X.509-Zertifikate mit RSA-Schlüsseln. Dabei werden die Dateierweiterungen .cer, .crt und .der erkannt. Die Verifizierung von Zertifikatsketten erfolgt durch Safari, Mail, VPN und andere Programme.

Die Geräte unterstützen P12-Dateien (PKCS-Standard #12), die genau eine Identität enthalten. Dabei werden die Dateierweiterungen .p12 und .pfx erkannt. Wenn eine Identität installiert ist, wird der Benutzer zur Eingabe des Kennworts aufgefordert, das als Schutz der Identität dient.

Die für den Aufbau der Zertifikatskette zu einem vertrauenswürdigen Root-Zertifikat (Stammzertifikat) erforderlichen Zertifikate können manuell oder mithilfe von Konfigurationsprofilen installiert werden. Sie müssen keine Root-Zertifikate hinzufügen, da diese von Apple auf dem Gerät installiert wurden. Eine Liste der bereits installierten Root-Zertifikate des Systems finden Sie im folgenden Apple-Support-Artikel: http://support.apple.com/kb/HT3580.

Zertifikate können auf Basis von SCEP auch bei drahtloser Verbindung sicher installiert werden. Weitere Informationen finden Sie im Abschnitt „Übersicht über die authentifizierte Registrierung und Konfiguration“ auf Seite 26.

E-Mail-Accounts

iPhone, iPod touch und iPad unterstützen standardkonforme IMAP4- und POP3-fähige Mail-Lösungen auf einer Reihe von Serverplattformen wie Windows, UNIX, Linux und Mac OS X. Mithilfe von IMAP können Sie über andere Exchange-Accounts auf Ihre E-Mail zugreifen (zusätzlich zu dem Exchange-Account, den Sie für den Direct Push-Dienst verwenden).

Führt ein Benutzer eine Suche in den eigenen Mail-Nachrichten aus, hat er die Möglichkeit, die Suche auf den Mail-Server auszuweiten. Diese Möglichkeit besteht bei Microsoft Exchange Server 2007
und den meisten IMAP-basierten Accounts.

Die Informationen des benutzereigenen E-Mail-Accounts (einschließlich der Benutzer-ID und des Kennworts für Exchange) werden auf sichere Weise auf dem Gerät gespeichert.

LDAP-Server

iPhone, iPod touch und iPad sind in der Lage, Kontaktinformationen aus den Unternehmensverzeichnissen eines LDAPv3-Servers in Ihrem Unternehmen abzurufen. Der Zugriff auf diese Verzeichnisse kann erfolgen, wenn Sie Ihre Kontaktinformationen durchsuchen, und er erfolgt automatisch, während Sie E-Mail-Adressen eingeben.

CalDAV-Server

iPhone, iPod touch und iPad können Kalenderdaten mit dem CalDAV-Server Ihres Unternehmens synchronisieren. Änderungen im Kalender werden in regelmäßigen Abständen zwischen dem Gerät und dem Server synchronisiert.

Zusätzlich können im Lesezugriff verfügbare Kalender abonniert werden (zum Beispiel ein Urlaubskalender oder der Terminkalender einer Kollegin oder eines Kollegen).

Das Erstellen und Senden neuer Kalendereinladungen auf dem Gerät wird für CalDAV-Accounts nicht unterstützt.

Zusätzliche Informationsressourcen

Neben diesem Handbuch enthalten auch die folgenden Veröffentlichungen und Websites nützliche Informationen:

- Webseite „iPhone in Unternehmen“ unter der Adresse: www.apple.com/de/iphone/enterprise
- Webseite „iPad in Unternehmen“ unter der Adresse: www.apple.com/de/ipad/business/
- Übersicht über Exchange Server unter der Adresse: http://technet.microsoft.com/en-us/library/bb124558.aspx bzw. http://technet.microsoft.com/de-de/library/bb124558.aspx
- Implementieren von Exchange ActiveSync unter der Adresse: http://technet.microsoft.com/en-us/library/aa995962.aspx bzw. http://technet.microsoft.com/de-de/library/aa995962.aspx
- Technische Dokumentation für Exchange 2003 unter der Adresse: http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx bzw. http://technet.microsoft.com/de-de/library/bb123872(EXCHG.65).aspx
- Verwalten von Exchange ActiveSync-Sicherheit unter der Adresse: http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx bzw. http://technet.microsoft.com/de-de/library/bb232020(EXCHG.80).aspx
- Webseite „Wi-Fi for Enterprise“ unter der Adresse: www.wi-fi.org/enterprise.php
- Webseite „Apple iPhone VPN Connectivity to Cisco Adaptive Security Appliances (ASA)“ unter der Adresse: www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html

- *iPhone-Benutzerhandbuch*, verfügbar unter der Adresse: www.apple.com/de/support/iphone/. Möchten Sie das Handbuch auf dem iPhone anzeigen, tippen Sie auf das Lesezeichen für das iPhone-Benutzerhandbuch in Safari oder besuchen Sie die Seite http://support.apple.com/de_DE/manuals/iphone/.
- iPhone-Videotour unter der Adresse: www.apple.com/de/iphone/guidedtour/
- *iPod touch-Benutzerhandbuch*, verfügbar unter der Adresse: www.apple.com/de/support/ipodtouch. Möchten Sie das Handbuch auf dem iPod touch anzeigen, tippen Sie auf das Lesezeichen für das iPod touch-Benutzerhandbuch in Safari oder besuchen Sie die Seite http://support.apple.com/de_DE/manuals/ipodtouch/.
- iPod touch-Videotour unter der Adresse: www.apple.com/de/ipodtouch/guidedtour/
- *iPad-Benutzerhandbuch*, verfügbar unter der Adresse: www.apple.com/de/support/ipad. Möchten Sie das Handbuch auf dem iPad anzeigen, tippen Sie auf das Lesezeichen für das iPad-Benutzerhandbuch in Safari oder besuchen Sie die Seite http://support.apple.com/de_DE/manuals/ipad/.
- iPad-Videotour unter der Adresse: www.apple.com/ipad/guided-tours/

Implementieren von iPhone- und iPod touch-Geräten

1

Dieses Kapitel enthält einen Überblick über die Implementierung von iPhone, iPod touch und iPad Ihrem Unternehmen.

iPhone, iPod touch und iPad lassen sich auf einfache Weise in Unternehmenssysteme wie Microsoft Exchange 2003 und 2007 sowie in drahtlose, sichere 802.1X-konforme Netzwerke und Cisco IPSec virtuelle private Netzwerke (VPNs) integrieren. Wie bei allen Unternehmenslösungen wird die Integration durch eine gute Planung und eine umfassende Kenntnis der verfügbaren Implementierungsoptionen vereinfacht und damit auch effizienter für Sie und Ihre Benutzer.

Bei der Planung der Implementierung von iPhone, iPod touch und iPad sollten die folgenden Aspekte berücksichtigt werden:

- Wie werden die iPhone- und iPad- (Wi-Fi + 3G Modelle) Geräte Ihres Unternehmens für den Mobilfunkdienst aktiviert?
- Auf welche Netzwerkdienste, Programme und Daten Ihres Unternehmens sollen die Benutzer zugreifen können?
- Welche Richtlinien (Policies) möchten Sie für die Geräte festlegen, um sensible Unternehmensdaten zu schützen?
- Sollen die Geräte einzeln und manuell konfiguriert werden, oder möchten Sie einen vereinheitlichten Prozess für die Konfiguration mehrerer Geräte nutzen?

Die individuellen Charakteristika Ihrer Unternehmensumgebung, die IT-Richtlinien, der Mobilfunkanbieter sowie die System- und Kommunikationsanforderungen bestimmen die geeignete Implementierungsstrategie.

Aktivieren der Geräte

Jedes iPhone muss von Ihrem Mobilfunkanbieter aktiviert werden, bevor es zum Empfangen und Tätigen von Anrufen, zum Versenden von Textnachrichten (SMS) oder zur Verbindung mit einem mobilen Datennetz genutzt werden kann. Informationen zu den Sprach- und Datentarifen sowie Anleitungen zur Aktivierung für Privat- und Geschäftskunden erhalten Sie bei Ihrem Mobilfunkanbieter.

Sie bzw. die Benutzer installieren zunächst eine SIM-Karte im iPhone. Anschließend muss das iPhone an einen Computer angeschlossen werden, auf dem iTunes installiert ist, um den Aktivierungsprozess abzuschließen. Ist die SIM-Karte bereits aktiviert, kann das iPhone sofort verwendet werden. Andernfalls werden Sie von iTunes schrittweise durch den Aktivierungsprozess für eine Reihe neuer Dienste geführt.

Das iPad muss mit einem Computer, auf dem iTunes installiert ist, verbunden sein, damit das Gerät aktiviert werden kann. Wenn Sie das iPad Wi-Fi + 3G in den USA verwenden, registrieren Sie sich mit dem iPad für einen AT&T-Mobilfunkvertrag. Anschließend können Sie die Mobilfunkdienste nutzen (oder den Vertrag beenden). Wählen Sie „Einstellungen“ > „Mobile Daten“ > „Account anzeigen“. Das iPad wird ohne Vertragsbindung geliefert. Wenden Sie sich an den Anbieter, um einen Account einzurichten und eine kompatible Mikro-SIM-Karte zu kaufen. In den USA gehören Mikro-SIM-Karten, die mit AT&T kompatibel sind, zum Lieferumfang des iPad Wi-Fi + 3G.

Obwohl es für den iPod touch und das iPad Wi-Fi keinen Mobilfunkdienst bzw. keine SIM-Karte gibt, muss das Gerät zur Aktivierung dennoch an einen Computer mit iTunes angeschlossen werden.

Da zum Abschließen des Aktivierungsprozesses das Programm „iTunes“ erforderlich ist, müssen Sie sich entscheiden, ob Sie iTunes auf allen Mac-Computern bzw. PCs der Benutzer installieren möchten, oder ob Sie die Aktivierung aller Geräte mit Ihrer eigenen iTunes-Installation abschließen möchten.

Für die Nutzung des Geräts in Verbindung mit Ihren Unternehmenssystemen ist iTunes im Anschluss an die Aktivierung nicht mehr erforderlich. Die Software wird allerdings benötigt, um Musik, Videos und Browser-Lesezeichen mit einem Computer zu synchronisieren. Auch zum Laden und Installieren von Softwareaktualisierungen für die Geräte sowie zum Installieren Ihrer Unternehmensprogramme wird die Software benötigt.

Weitere Informationen über das Aktivieren von Geräten und die Verwendung von iTunes finden Sie in Kapitel 4.

Vorbereiten des Zugriffs auf Netzwerkdienste und Unternehmensdaten

Die iPhone OS 3.x-Software unterstützt das sichere, sofortige Weiterleiten von E-Mail, Kontaktinformationen und Kalenderereignissen über Microsoft Exchange Server 2003 oder 2007 (Push-Dienste) sowie GAL (Global Address Lookup), Fernlöschen (Remote Wipe) und die Richtlinie zur zwingenden Eingabe des Gerätecodes. Darüber hinaus können die Benutzer über WPA Enterprise- und WPA2 Enterprise-Funknetzwerke mithilfe der 802.1 X-Identifizierung und/oder über VPN unter Verwendung der Protokolle PPTP, LT2P over IPSec bzw. Cisco IPSec eine sichere Verbindung zu den Unternehmensressourcen herstellen.

Wenn Microsoft Exchange in Ihrem Unternehmen nicht verwendet wird, können die Benutzer trotzdem mit dem iPhone bzw. dem iPod touch arbeiten, um mit den meisten standardkonformen POP- oder IMAP-basierten Servern und Diensten E-Mails drahtlos zu synchronisieren. Mithilfe von iTunes können die Benutzer auch ihre Kalendereignisse und Kontaktinformationen aus Mac OS X iCal und dem Adressbuch bzw. Microsoft Outlook auf einem Windows-PC synchronisieren. Für den drahtlosen Zugriff auf Kalender und Verzeichnisse werden CalDAV und LDAP unterstützt.

Berücksichtigen Sie bei Ihren Überlegungen, auf welche Netzwerkdienste Benutzer Zugriff erhalten sollen, die Informationen in den folgenden Abschnitten.

Microsoft Exchange

Das iPhone kommuniziert über Microsoft Exchange ActiveSync (EAS) direkt mit Ihrem Microsoft Exchange Server. Exchange ActiveSync hält eine Verbindung zwischen dem Exchange Server und dem iPhone oder iPad Wi-Fi + 3G aufrecht, damit das Gerät beim Eintreffen einer neuen E-Mail-Nachricht oder einer Einladung zu einer Besprechung sofort aktualisiert werden kann. Da für iPod touch und iPad Wi-Fi keine permanente Mobilfunkverbindung besteht, wird das Gerät nur über die Verfügbarkeit neuer Daten informiert, wenn es aktiv und mit einem Wi-Fi-Netzwerk verbunden ist.

Wenn Ihr Unternehmen Exchange ActiveSync für Exchange Server 2003 oder Exchange Server 2007 unterstützt, stehen Ihnen die erforderlichen Dienste bereits zur Verfügung. Unter Exchange Server 2007 ist sicherzustellen, dass die ClientAccess-Funktion installiert ist. Unter Exchange Server 2003 ist sicherzustellen, dass Outlook Mobile Access (OMA) aktiviert ist.

Wenn Sie einen Exchange Server verwenden, Ihr Unternehmen mit Exchange ActiveSync aber noch wenig Erfahrung hat, lesen Sie die Informationen in den folgenden Abschnitten.

Netzwerkkonfiguration

- Stellen Sie sicher, dass Port 443 in der Firewall geöffnet ist. Wenn Ihr Unternehmen Outlook Web Access verwendet, ist Port 443 wahrscheinlich bereits geöffnet.
- Vergewissern Sie sich, dass auf dem Exchange Frontend-Server ein Serverzertifikat installiert ist, und aktivieren Sie als einzige Authentifizierungsmethode die Standardauthentifizierung, damit für die Verbindung zum Microsoft Server ActiveSync-Verzeichnis Ihres IIS eine SSL-Verschlüsselung erfolgt.
- Wird ein Microsoft ISA-Server (Internet Security and Acceleration) verwendet, muss geprüft werden, ob ein Serverzertifikat installiert ist. Aktualisieren Sie den DNS-Server, damit eingehende Verbindungen richtig aufgelöst werden.
- Stellen Sie sicher, dass der DNS-Server für Ihr Netzwerk sowohl für Intranet- als auch für Internet-Clients eine einzelne, extern weiterleitbare IP-Adresse an den Exchange ActiveSync-Server übergibt. Dies ist erforderlich, damit das Gerät die gleiche IP-Adresse für die Kommunikation mit dem Server verwenden kann, auch wenn beide Verbindungsarten aktiv sind.
- Wird ein Microsoft ISA-Server verwendet, müssen ein Web-Listener und eine Bereitstellungsrichtlinie für den Zugriff durch Exchange Web-Clients erstellt werden. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
- Legen Sie für alle Firewalls und Netzwerk-Appliances das Zeitlimit (Timeout) für inaktive Sitzungen auf 30 Minuten fest. In der Dokumentation zu Microsoft Exchange finden Sie unter der folgenden Adresse weitere Informationen über Taktintervalle und Zeitlimits: http://technet.microsoft.com/en-us/library/cc182270.aspx.

Konfigurieren des Exchange-Accounts

- Aktivieren Sie Exchange ActiveSync mithilfe des Active Directory-Diensts für bestimmte Benutzer oder Gruppen. Die Aktivierung erfolgt unter Exchange Server 2003 und Exchange Server 2007 auf Organisationsebene standardmäßig für alle mobilen Geräte (vgl. Empfängerkonfiguration der Exchange-Verwaltungskonsole unter Exchange 2007).
- Konfigurieren Sie mithilfe des Exchange-System-Managers die Funktionen für mobile Geräte, die Richtlinien und die Einstellungen für die Gerätesicherheit. Unter Exchange Server 2007 können diese Einstellungen über die Exchange-Verwaltungskonsole vorgenommen werden.
- Laden und Installieren Sie das Microsoft Exchange ActiveSync Mobile Administration Web Tool, das zum Löschen von mobilen Geräten per Fernzugriff (Remote Wipe) erforderlich ist. Unter Exchange Server 2007 kann Remote Wipe auch mithilfe von Outlook Web Access oder über die Exchange-Verwaltungskonsole gestartet werden.

WPA/WPA2 Enterprise-Wi-Fi-Netzwerke

Die Unterstützung für WPA Enterprise und WPA2 Enterprise gewährleistet den sicheren Zugriff auf drahtlose Unternehmensnetzwerke über iPhone, iPod touch und iPad. WPA/WPA2 Enterprise arbeitet mit einer AES-128-Bit-Verschlüsselung, einem bewährten, blockbasierten Verschlüsselungsverfahren, das ein hohes Maß an Sicherheit für die Unternehmensdaten bietet.

Da die 802.1X-Identifizierung unterstützt wird, lassen sich iPhone OS-Geräte in eine Vielzahl von RADIUS-Serverumgebungen integrieren. Die 802.1X-Identifizierungsverfahren für Funknetze werden unterstützt und umfassen EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 und LEAP.

Konfigurieren des WPA/WPA2 Enterprise-Netzwerks

- Prüfen Sie die Netzwerk-Appliances auf Kompatibilität und wählen Sie einen Identifizierungstyp (EAP-Typ), der von iPhone, iPod touch und iPad unterstützt wird. Vergewissern Sie sich, dass 802.1X auf dem Identifizierungsserver aktiviert ist und installieren Sie gegebenenfalls ein Serverzertifikat und weisen Sie den Benutzern und Gruppen die entsprechenden Berechtigungen für den Netzwerkzugriff zu.
- Konfigurieren Sie die Funkzugangsknoten (WAP; Wireless Access Points) für die 802.1X-Identifizierung und geben Sie die entsprechenden Informationen für den RADIUS-Server ein.
- Testen Sie Ihre 802.1X-Implementierung mit einem Mac oder einem PC um sicherzustellen, dass die RADIUS-Identifizierung richtig konfiguriert ist.
- Wenn Sie beabsichtigen, eine zertifikatbasierte Identifizierung zu verwenden, muss sichergestellt sein, dass die Infrastruktur für den öffentlichen Schlüssel so konfiguriert ist, dass geräte- und benutzerbasierte Zertifikate vom entsprechenden Schlüsselverteilungsprozess unterstützt werden.
- Überprüfen Sie die Kompatibilität Ihrer Zertifikatformate mit dem Gerät und mit Ihrem Identifizierungsserver. Weitere Informationen über Zertifikate finden Sie im Abschnitt „Zertifikate und Identitäten“ auf Seite 13.

VPNs (Virtual Private Networks)

Der sichere Zugriff auf private Netzwerke wird von iPhone, iPod touch und iPad mithilfe der VPN-Protokolle Cisco IPSec, L2TP over IPSec und PPTP sichergestellt. Wenn Ihr Unternehmen eines dieser Protokolle unterstützt, ist für die Verwendung Ihrer Geräte in einer VPN-Infrastruktur keine zusätzliche Netzwerkkonfiguration oder Software von Drittanbietern erforderlich.

Cisco IPSec-Implementierungen können die Vorteile der zertifikatbasierten Identifizierung über standardkonforme X.509-Zertifikate nutzen. Auf der Basis der zertifikatbasierten Identifizierung können Sie außerdem die Vorteile von VPN On Demand nutzen, um eine sichere drahtlose Verbindung zu Ihrem Unternehmensnetzwerk herzustellen.

Für die tokenbasierte Zwei-Faktor-Identifizierung unterstützt das iPhone OS RSA SecurID und CryptoCard. Die Benutzer geben ihre PIN und ein vom Token generiertes Einmalkennwort direkt auf dem Gerät ein, wenn sie die VPN-Verbindung herstellen. In Anhang A finden Sie kompatible Cisco-VPN-Server sowie Konfigurationsempfehlungen.

iPhone, iPod touch und iPad unterstützen auch die Shared-Secret-Identifizierung für Cisco IPSec- und L2TP/IPSec-Implementierungen sowie MS-CHAPv2 für die einfache Identifizierung mithilfe von Benutzername und Kennwort.

Außerdem wird auch die automatische VPN-Proxy-Konfiguration (PAC und WPAD) unterstützt, mit der Sie die Proxy-Servereinstellungen für den Zugriff auf bestimmte URLs festlegen können.

Hinweise zur VPN-Konfiguration

- Das iPhone OS lässt sich in die meisten VPN-Netzwerke integrieren, sodass in der Regel nur ein minimaler Konfigurationsaufwand erforderlich ist, um den Zugriff auf Ihr Netzwerk über diese Geräte zu aktivieren. Zur Vorbereitung der Implementierung empfiehlt es sich, zunächst zu prüfen, ob die in Ihrem Unternehmen genutzten VPN-Protokolle und Identifizierungsverfahren von iPhone unterstützt werden.
- Stellen Sie sicher, dass Ihre VPN-Konzentratoren die erforderlichen Standards unterstützen. Es empfiehlt sich auch, den Identifizierungspfad zu Ihrem RADIUS- oder Identifizierungsserver zu prüfen, damit sichergestellt ist, dass die vom iPhone OS unterstützten Standards innerhalb Ihrer Implementierung aktiviert sind.
- Lassen Sie sich von Ihrem Lösungsanbieter bestätigen, dass Ihre Software und Ihre Geräteausstattung auf dem neuesten Stand ist und über die aktuellsten Sicherheits-Patches und die neueste Firmware verfügt.
- Wenn Sie die Proxy-Einstellungen für eine spezifische URL konfigurieren wollen, können Sie auf einem Webserver, auf den Sie basierend auf den grundlegenden VPN-Einstellungen zugreifen können, eine PAC-Datei ablegen und im Hinblick auf diese Datei den MIME-Typ „application/x-ns-proxy-autoconfig“ ergänzen. Alternativ können Sie Ihre DNS- oder DHCP-Konfiguration so gestalten, dass der Speicherort einer WPAD-Datei auf einem Server bereitgestellt wird, der auf ähnliche Weise zugänglich ist.

IMAP-E-Mail

Wenn Sie nicht mit Microsoft Exchange arbeiten, können Sie trotzdem eine sichere, standardbasierte E-Mail-Lösung implementieren. Hierfür können Sie beliebige Mail-Server verwenden, die IMAP unterstützen und so konfiguriert sind, dass eine Benutzeridentifizierung und die SSL-Verschlüsselung erforderlich sind. Mit dieser Technik können Sie beispielsweise auf Lotus Notes/Domino- oder Novell GroupWise-E-Mails zugreifen. Die Mail-Server können sich innerhalb eines DMZ-Teilnetzes und/oder hinter einer Unternehmensfirewall befinden.

Mit SSL unterstützt das iPhone OS die 128-Bit-Verschlüsselung sowie X.509-Zertifikate, die von führenden Zertifizierungsstellen ausgestellt werden. Es unterstützt darüber hinaus auch sichere Identifizierungsverfahren wie das standardkonforme MD5 Challenge-Response-Verfahren und NTLMv2.

Hinweise zur IMAP-Konfiguration

- Installieren Sie ein von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestelltes digitales Zertifikat auf dem Server, um zusätzliche Sicherheit zu erhalten. Das Installieren eines von einer Zertifizierungsstelle ausgestellten Zertifikats ist ein wichtiger Schritt, der sicherstellt, dass Ihr Proxy-Server innerhalb Ihrer Unternehmensinfrastruktur eine vertrauenswürdige Einheit darstellt. Im Abschnitt „Einstellungen im Bereich „Zertifikate““ auf Seite 44 finden Sie weitere Informationen zur Installation von Zertifikaten auf dem iPhone.
- Damit iPhone OS-Geräte E-Mails von Ihrem Server abrufen können, muss Port 993 in der Firewall geöffnet werden. Stellen Sie auch sicher, dass der Proxy-Server auf „IMAP über SSL“ eingestellt ist.
- Damit die Geräte E-Mails senden können, müssen die Ports 587, 465 oder 25 geöffnet sein. Da Port 587 zuerst verwendet wird, ist er die beste Wahl.

LDAP-Verzeichnisse

iPhone OS ermöglicht den Zugriff auf standardbasierte LDAP-Verzeichnisserver und stellt ein globales Adressverzeichnis oder andere Informationen bereit, die mit der globalen Adressliste (GAL) von Microsoft Exchange vergleichbar sind.

Wenn Sie auf dem Gerät einen LDAP-Account konfigurieren, sucht das Gerät auf der Root-Ebene des Servers nach dem Attribut `namingContexts`, um davon ausgehend den standardmäßigen Suchbeginn zu identifizieren. Der Suchbereich ist standardmäßig auf „Subtree“ (Teilbaum) eingestellt.

CalDAV-Kalender

Mithilfe der in iPhone OS integrierten CalDAV-Unterstützung können in Umgebungen ohne Microsoft Exchange-Installation Kalender- und Zeitplanfunktionen auf globaler Ebene bereitgestellt werden. Das iPhone OS kann für alle Kalenderserver genutzt werden, die den CalDAV-Standard unterstützen.

Abonnierte Kalender

Wenn Kalender für unternehmensspezifische Ereignisse (zum Beispiel Urlaube und besondere Veranstaltungen) veröffentlicht und mit Lesezugriff bereitgestellt werden, können Sie diese Kalender auf iPhone OS-Geräten abonnieren und sie zusammen mit den Microsoft Exchange- und CalDAV-Kalendern anzeigen. Das iPhone OS unterstützt alle Kalenderdateien, die im iCalendar-Standardformat (.ics) vorliegen.

Eine einfache Möglichkeit, abonnierte Kalender an Ihre Benutzer weiterzugeben, besteht darin, ihnen per SMS oder E-Mail die vollständig qualifizierte URL-Adresse zu senden. Tippt der Benutzer auf den Link, bieten die Geräte die Möglichkeit, den angegebenen Kalender zu abonnieren.

Unternehmensprogramme

Wenn Sie iPhone OS-Unternehmensprogramme bereitstellen wollen, können Sie diese Programme mithilfe des iPhone-Konfigurationsprogramms oder mit iTunes auf den Geräten installieren. Wenn Sie ein Programm auf den Geräten der Benutzer implementieren, ist die Aktualisierung dieser Programme einfacher, wenn die Benutzer iTunes auf ihrem Mac oder PC installiert haben.

OSCP (Online Certificate Status Protocol)

Wenn Sie digitale Zertifikate für iPhone OS-Geräte bereitstellen, überlegen Sie, sie als OCSP-fähige Zertifikate auszugeben. Das Gerät kann dann vor der Verwendung des Zertifikats bei Ihrem OCSP-Server anfragen, ob das Zertifikat widerrufen wurde.

Festlegen der Richtlinien für den Gerätecode

Nachdem Sie festgelegt haben, auf welche Netzwerkdienste und Daten Ihre Benutzer zugreifen sollen, müssen Sie die Richtlinien für den Gerätecode definieren.

Unternehmen, deren Netzwerke, Systeme oder Programme kein Kennwort und kein Identifizierungs-Token erfordern, wird empfohlen, die Festlegung eines Codes auf den Geräten zwingend zu erfordern. Wenn Sie eine zertifikatbasierte Identifizierung für ein 802.1X-Netzwerk oder Cisco IPSec-VPN verwenden, oder wenn Ihr Unternehmensprogramm Ihre Anmeldedaten speichert, sollten Sie Ihre Benutzer auffordern, einen Gerätecode mit einem kurzen Intervall für die Zeitabschaltung festzulegen, damit ein verloren gegangenes oder gestohlenes Gerät ohne den Gerätecode nicht verwendet werden kann.

Richtlinien können auf dem iPhone, iPod touch und iPad auf zwei verschiedene Arten festgelegt werden. Ist das Gerät für den Zugriff auf einen Microsoft Exchange-Account konfiguriert, werden die Exchange ActiveSync-Richtlinien drahtlos an das Gerät übermittelt. In diesem Fall können Sie die Richtlinien ohne Benutzeraktion durchsetzen und aktualisieren. Weitere Informationen zu den EAS-Richtlinien finden Sie im Abschnitt „Unterstützte Exchange ActiveSync-Richtlinien (Policies)“ auf Seite 9.

Wenn Sie nicht mit Microsoft Exchange arbeiten, können Sie auf Ihren Geräten ähnliche Richtlinien festlegen, indem Sie Konfigurationsprofile erstellen. Wenn Sie Änderungen an einer Richtlinie vornehmen, müssen Sie den Benutzern ein entsprechend aktualisiertes Profil bereitstellen oder ihnen zusenden oder alternativ das geänderte Profil mithilfe des iPhone-Konfigurationsprogramms installieren. Weitere Informationen zu den Richtlinien für den Gerätecode finden Sie im Abschnitt „Einstellungen im Bereich „Code““ auf Seite 37.

Wenn Sie Microsoft Exchange verwenden, können Sie Ihre EAS-Richtlinien auch durch die Verwendung von Konfigurationsrichtlinien ergänzen. Dadurch wird beispielsweise der Zugriff auf Richtlinien möglich, die unter Microsoft Exchange 2003 nicht zur Verfügung stehen, oder Sie können Richtlinien speziell für das iPhone OS definieren.

Konfigurieren von Geräten

Sie müssen für jedes einzelne iPhone-, iPod touch und iPad-Gerät festlegen, wie es konfiguriert werden soll. Dabei spielt eine Rolle, wie viele Geräte Sie implementieren und verwalten möchten. Handelt es sich um eine geringe Anzahl von Geräten, ist es unter Umständen einfacher, wenn Sie oder Ihre Benutzer die Geräte manuell konfigurieren. Die Einstellungen für jeden Mail-Account, die Wi-Fi-Einstellungen und die VPN-Konfigurationsdaten werden in diesem Fall direkt am Gerät eingegeben. In Kapitel 3 finden Sie ausführliche Informationen über die manuelle Konfiguration.

Wenn Sie eine größere Anzahl von Geräten implementieren möchten, oder zahlreiche E-Mail- und Netzwerk-Einstellungen festlegen und Zertifikate installieren müssen, empfiehlt es sich, die Geräte zu konfigurieren, indem Konfigurationsprofile erstellt und verteilt werden. Mit Konfigurationsprofilen können Einstellungen und Identifizierungsinformationen schnell auf das Gerät geladen werden. Einige VPN- und Wi-Fi-Einstellungen können ausschließlich über ein Konfigurationsprofil festgelegt werden. Wenn Sie nicht mit Microsoft Exchange arbeiten, müssen Sie auch zum Festlegen des Gerätecodes ein Konfigurationsprofil verwenden.

Konfigurationsprofile können verschlüsselt und signiert werden. Dies gibt Ihnen die Möglichkeit, den Einsatz eines Profils auf ein bestimmtes Gerät zu beschränken und Änderungen an den Einstellungen des Profils durch Dritte zu verhindern. Sie können ein Profil auf dem Gerät auch als geschützt markieren. In diesem Fall kann das Profil nach der Installation nur gelöscht werden, indem alle Daten vom Gerät gelöscht werden oder alternativ ein administrativer Code eingegeben wird.

Unabhängig davon, ob Sie die Geräte manuell oder mithilfe von Konfigurationsprofilen konfigurieren, muss auch festgelegt werden, ob Sie die Geräte selbst konfigurieren oder ob Sie diese Aufgabe Ihren Benutzern übertragen. Dies hängt davon ab, wo sich Ihre Benutzer befinden, welche Unternehmensrichtlinien es für die Verwaltung von IT-Ausrüstung durch die Benutzer gibt, und wie komplex die Gerätekonfiguration ist, die Sie implementieren möchten. Konfigurationsprofile eignen sich besonders für große Unternehmen, für Außendienstmitarbeiter und für Benutzer, die ihre Geräte nicht selbst einrichten können.

Sollen die Benutzer ihre Geräte selbst aktivieren oder sollen Unternehmensprogramme installiert oder aktualisiert werden, muss iTunes auf dem Mac oder PC der Benutzer installiert sein. iTunes ist auch für Aktualisierungen der iPhone OS-Software erforderlich. Bitte bedenken Sie dies, wenn Sie entscheiden, iTunes nicht an Ihre Benutzer zu verteilen. Weitere Informationen zur Implementierung und Bereitstellung von iTunes finden Sie in Kapitel 4.

Drahtlose Registrierung und Konfiguration

Als *Registrierung* wird der Prozess bezeichnet, mit dem ein Gerät und ein Benutzer mit dem Ziel identifiziert werden, die Verteilung von Zertifikaten zu automatisieren. Digitale Zertifikate bieten viele Vorteile für Benutzer. Sie werden zum Beispiel für die Identifizierung eines Benutzers verwendet, wenn er versucht, auf zentrale Dienste eines Unternehmens oder einer Organisation wie Microsoft Exchange ActiveSync, drahtlose WPA2 Enterprise-Netzwerke oder VPN-Verbindungen zum Unternehmensnetzwerk zuzugreifen. Die zertifikatbasierte Identifizierung ermöglicht außerdem den Einsatz von VPN On Demand für den nahtlosen Zugang zu Unternehmensnetzwerken.

Zusätzlich zu der Option, Zertifikate für die PKI (Public Key Infrastructure) Ihres Unternehmens mit den Mitteln der drahtlosen Identifizierung zu verteilen, haben Sie auch die Möglichkeit, spezielle Profile für die Gerätekonfiguration bereitzustellen und zu implementieren. Auf diese Weise ist sichergestellt, dass nur vertrauenswürdige Benutzer auf die Dienste Ihres Unternehmens zugreifen und dass deren Geräte gemäß Ihren IT-Richtlinien konfiguriert sind. Da Konfigurationsprofile verschlüsselt und geschützt werden können, bieten sie außerdem den Vorteil, dass ihre Einstellungen weder gelöscht noch geändert oder an andere Benutzer weitergegeben werden können. Die genannten Möglichkeiten stehen beim unten beschriebenen drahtlosen Prozess und auch im iPhone-Konfigurationsprogramm zur Verfügung, solange das konfigurierte Gerät mit Ihrem Administrationscomputer verbunden ist. Weitere Informationen über das iPhone-Konfigurationsprogramm finden Sie in Kapitel 2.

Die Implementierung der drahtlosen Identifizierung und Konfiguration erfordert die Entwicklung und Integration von Identifizierungs-, Verzeichnis- und Zertifizierungsdiensten. Die Bereitstellung und Implementierung kann mithilfe standardmäßiger Webdienste erfolgen. Nachdem alle notwendigen Voraussetzungen geschaffen wurden, können Benutzer ihre Geräte in einer sicheren, authentifizierten Umgebung einrichten.

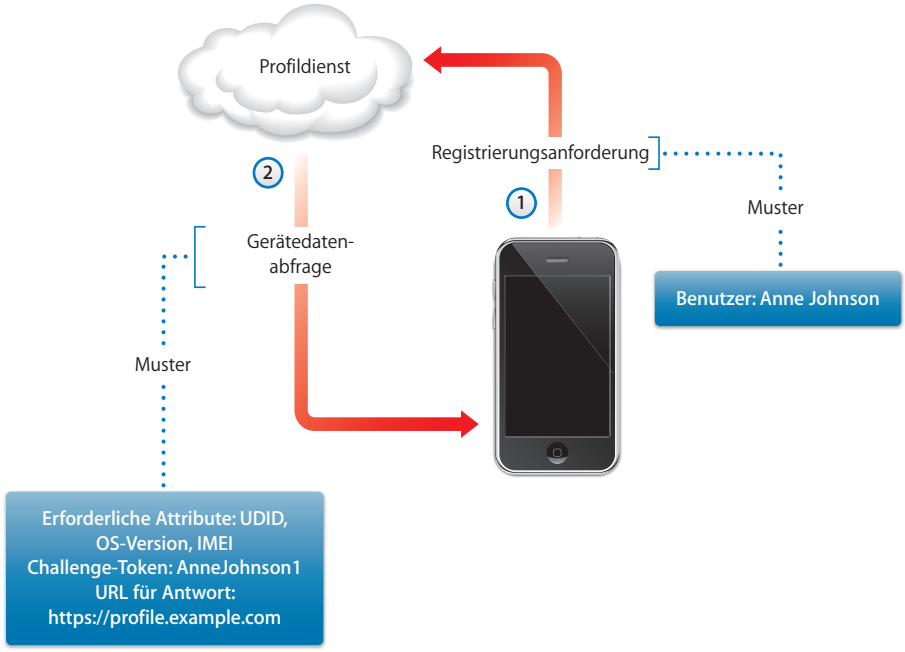
Übersicht über die authentifizierte Registrierung und Konfiguration

Für die Implementierung dieses Prozesses müssen Sie einen eigenen *Profilweitergabedienst* erstellen, der HTTP-Verbindungen, die Identifizierung von Benutzern, das Erstellen von mobileconfig-Profilen und die Verwaltung des im Folgenden beschriebenen Gesamtprozesses unterstützt.

Außerdem benötigen Sie eine Zertifizierungsstelle (Certificate Authority, CA), damit Sie Ihre gerätespezifischen Zertifikate mithilfe des Protokolls SCEP (Simple Certificate Enrollment Protocol) bereitstellen können. Links zu PKI, SCEP und zugehörigen Themen finden Sie unter „Weitere Informationsquellen“ auf Seite 31.

Das folgende Diagramm zeigt den vom iPhone unterstützten Registrierungs- und Konfigurationsprozess.

Phase 1 – Beginn der Registrierung

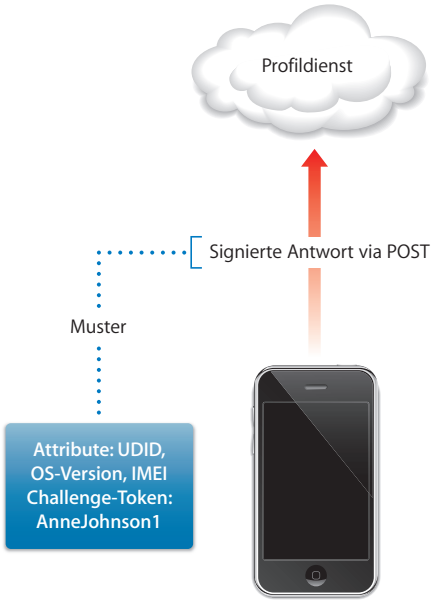


Phase 1 – Beginn der Registrierung: Die Registrierung beginnt damit, dass der Benutzer in Safari auf die URL des von Ihnen erstellten Profilweitergabedienst zugreift. Sie können diese URL per SMS oder E-Mail weitergeben. Mit der Registrierungsanforderung, im Diagramm oben als Schritt 1 dargestellt, sollte die Identität des Benutzers authentifiziert werden. Für die Authentifizierung und Identifizierung genügt unter Umständen eine einfache Identifizierung (basic auth). Sie können aber auch vorhandene Verzeichnisdienste heranziehen.

In Schritt 2 sendet Ihr Dienst als Antwort auf die Anforderung ein Konfigurationsprofil (.mobileconfig). Diese Antwort umfasst eine Liste von Attributen, die das Gerät mit seiner nächsten Antwort senden muss, sowie einen Pre-Shared Key (PSK), d. h. ein vorab ausgetauschtes Kennwort zur Authentifizierung, als so genannte Challenge. Mithilfe des PSK kann die Identität des Benutzers über den gesamten Prozess aufrecht erhalten werden, was Ihnen die Möglichkeit gibt, den Konfigurationsprozess individuell für jeden Benutzer anzupassen. Zu den Geräteattributen, die angefordert werden können, gehören die iPhone OS-Version, die Geräte-ID (MAC-Adresse), der Produkttyp (das iPhone 3GS wird als iPhone2,1 angegeben), die Telefon-ID (IMEI) und die SIM-Angaben (ICCID).

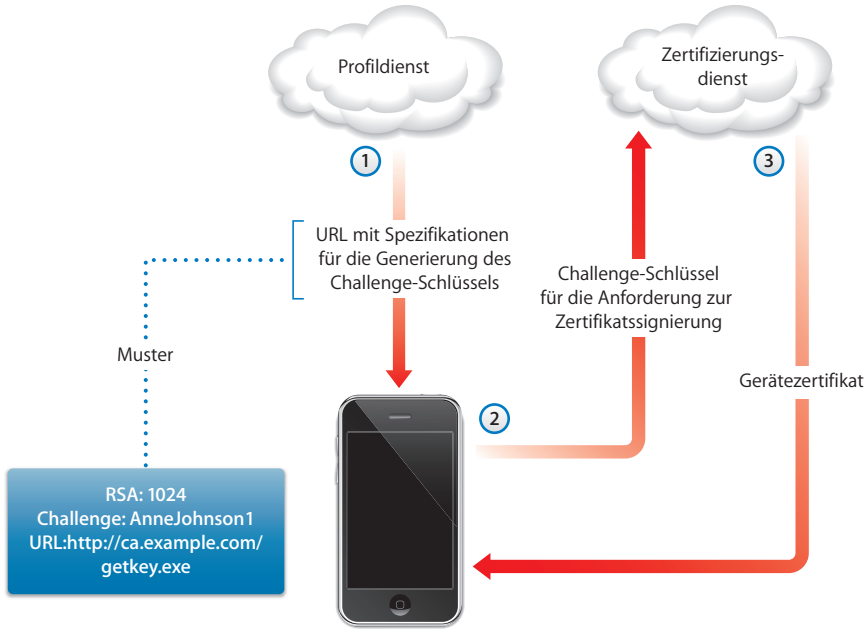
Im Abschnitt „Muster für Phase 1 – Antwort des Servers“ auf Seite 98 sehen Sie ein Beispiel für ein Konfigurationsprofil in dieser Phase.

Phase 2 – Identifizierung des Geräts



Phase 2 – Identifizierung des Geräts: Wenn sich der Benutzer mit der Installation des in Phase 1 empfangenen Profils einverstanden erklärt, sucht das Gerät nach den angeforderten Attributen, fügt gegebenenfalls die Antwort auf die Challenge hinzu und signiert die Antwort mit der in das Gerät integrierten Identität. (Hierbei handelt es sich um ein von Apple ausgegebenes Zertifikat.) Abschließend wird die Antwort per HTTP Post an den Profilweitergabedienst zurück gesendet.

Im Abschnitt „Muster für Phase 2 – Antwort des Geräts“ auf Seite 99 sehen Sie ein Beispiel für ein Konfigurationsprofil in dieser Phase.



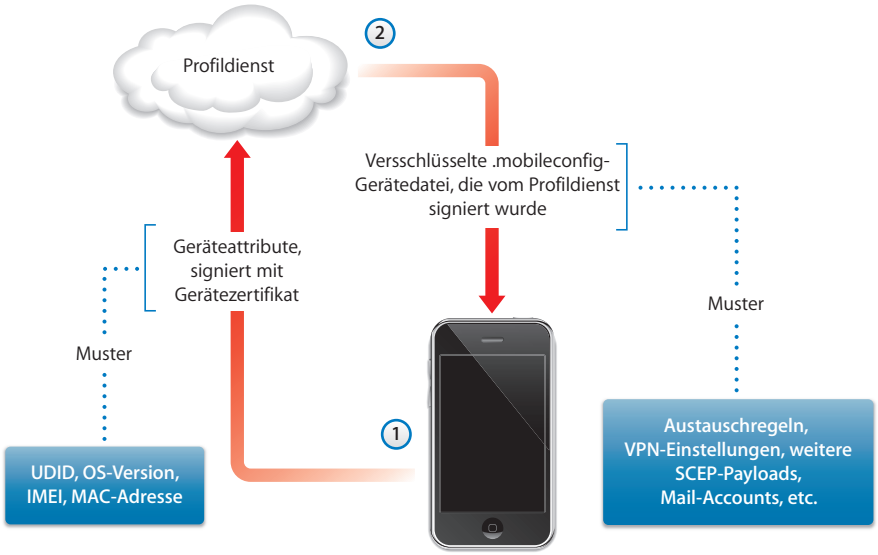
Phase 3 – Installation des Zertifikats: In Schritt 1 sendet der Profilweitergabedienst eine Antwort mit Spezifikationen, auf deren Basis das Gerät nun einen Schlüssel generiert (RSA 1024), sowie Angaben dazu, wohin diese Schlüsseldaten für die Zertifizierung mit SCEP (Simple Certificate Enrollment Protocol) gesendet werden müssen.

In Schritt 2 muss die SCEP-Anforderung automatisch bearbeitet werden. Dies ist möglich, da für die Authentifizierung/Identifizierung der Anforderung die Challenge-Informationen im SCEP-Paket verwendet werden.

In Schritt 3 liefert die Zertifizierungsstelle (CA) als Antwort ein Verschlüsselungszertifikat für das Gerät.

Im Abschnitt „Muster für Phase 3 – Antwort des Servers mit SCEP-Spezifikationen“ auf Seite 99 sehen Sie ein Beispiel für ein Konfigurationsprofil in dieser Phase.

Phase 4 – Gerätekonfiguration



Phase 4 – Konfigurierung des Geräts: In Schritt 1 sendet das Gerät eine Liste von Attributen, die mithilfe des Verschlüsselungszertifikats signiert ist, das in der vorherigen Phase von der Zertifizierungsstelle (CA) bereitgestellt wurde.

In Schritt 2 sendet der Profildienst im Gegenzug eine verschlüsselte .mobileconfig-Datei, die automatisch installiert wird. Diese .mobileconfig-Datei muss vom Profildienst signiert werden. Für diesen Zweck kann zum Beispiel dessen SSL-Zertifikat verwendet werden.

Außer den allgemeinen Einstellungen sollte dieses Konfigurationsprofil auch die Richtlinien Ihres Unternehmens definieren, deren Umsetzung und Anwendung erzwungen werden sollten. Außerdem sollte das Profil geschützt werden, damit der Benutzer es nicht vom Gerät entfernen kann. Das Konfigurationsprofil kann zusätzliche Anforderungen bezüglich der Registrierung von Identitäten per SCEP enthalten. Diese Anforderungen werden im Zuge der Installation des Profils ausgeführt.

Bei einem Zertifikat, das mithilfe von SCEP installiert wurde und abläuft oder anderweitig ungültig wird, erhält der Benutzer die Aufforderung, das Profil zu aktualisieren. Bestätigt der Benutzer die Aufforderung, wiederholt das Gerät den oben beschriebenen Prozess, um ein neues Zertifikat und Profil zu erhalten.

Im Abschnitt „Muster für Phase 4 – Antwort des Geräts“ auf Seite 101 sehen Sie ein Beispiel für ein Konfigurationsprofil in dieser Phase.

Weitere Informationsquellen

- Digital Certificates PKI for IPSec VPNs.pdf unter der Adresse: https://cisco.hosted.jivesoftware.com/docs/DOC-3592
- Public-Key-Infrastructure unter der Adresse: http://de.wikipedia.org/wiki/Public_Key_Infrastructure
- Spezifikation für das Protokoll IETF SCEP unter der Adresse: http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt

Weitere Informationen und Ressourcen für iPhone, iPod touch und iPad in Unternehmen finden Sie unter der Adresse: www.apple.com/de/iphone/enterprise/ und www.apple.com/de/ipad/business/.

Erstellen und Implementieren von Konfigurationsprofilen

2

Konfigurationsprofile legen fest, wie iPhone, iPad und iPod touch in Ihre Unternehmensinstallationen eingebunden werden.

Konfigurationsprofile sind XML-Dateien, die gerätespezifische Sicherheitsrichtlinien und Einschränkungen, VPN-Konfigurationsinformationen, Wi-Fi-Einstellungen, Accounts für E-Mail- und Kalenderfunktionen und Identifizierungszertifikate enthalten, die es dem Gerät (iPhone, iPod touch und iPad) ermöglichen, mit den Systemen in Ihrem Unternehmen zu kommunizieren und zu kooperieren.

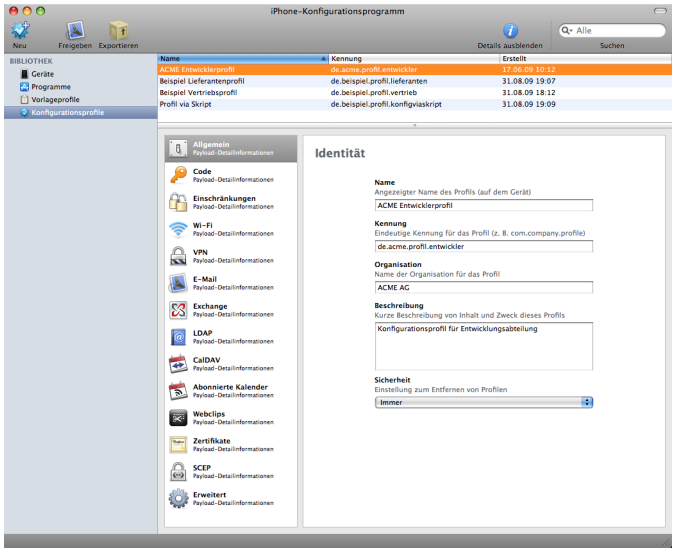
Sie können ein Konfigurationsprofil auf einem Gerät mithilfe des iPhone-Konfigurationsprogramms installieren. Dazu muss das Gerät über USB mit einem Computer verbunden sein. Alternativ können Sie Konfigurationsprofile per E-Mail verteilen o der auf einer Website bereitstellen. Wenn ein Benutzer den E-Mail-Anhang öffnet bzw. das Profil mithilfe von Safari auf sein Gerät lädt, wird er aufgefordert, den Installationsprozess zu starten.

Sollen keine Konfigurationsprofile erstellt und verteilt werden, können die Geräte auch manuell konfiguriert werden. Weitere Informationen hierzu finden Sie in Kapitel 3.

iPhone-Konfigurationsprogramm

Mit dem iPhone-Konfigurationsprogramm können Sie auf unkomplizierte Weise Konfigurationsprofile erstellen, verschlüsseln und installieren, Vorlageprofile und autorisierte Programme überwachen und installieren sowie Konsolenprotokolle und andere gerätespezifische Informationen erfassen. Mit dem Installationsprogramm für das iPhone-Konfigurationsprogramm wird das Programm unter Mac OS X im Ordner „/Programme/Dienstprogramme“ und unter Windows im Verzeichnis „Programme\iPhone Configuration Utility“ installiert.

Wenn Sie das Programm öffnen, wird ein ähnliches Fenster wie unten abgebildet angezeigt.



Der Inhalt des Hauptbereichs dieses Fensters ändert sich, wenn Sie Objekte in der Seitenleiste auswählen.

In der Seitenleiste wird die Bibliothek angezeigt, die folgende Kategorien enthält:

- Unter *Geräte* wird eine Liste der an den Computer angeschlossenen iPhone- und iPod touch-Geräte angezeigt.
- Unter *Programme* werden Programme aufgelistet, die auf den an den Computer angeschlossenen Geräten installiert werden können. Damit ein Programm auf einem Gerät ausgeführt werden kann, ist unter Umständen ein Vorlageprofil erforderlich.
- Unter *Profile bereitstellen* werden Vorlageprofile (Provisioning-Profile) angezeigt, die eine Verwendung des Geräts für die iPhone OS-Entwicklung erlauben (autorisiert durch die Apple Developer Connection). Weitere Informationen finden Sie in Kapitel 5. Mithilfe von Vorlageprofilen können auf Geräten außerdem auch unternehmensspezifische Programme ausgeführt werden, deren Verteilung nicht über den iTunes Store erfolgt.
- Im Bereich *Konfigurationsprofile* werden alle zuvor erstellten Konfigurationsprofile angezeigt. Sie können die festgelegten Informationen bearbeiten oder ein neues Konfigurationsprofil erstellen und es an einen Benutzer senden oder es auf einem angeschlossenen Gerät installieren.

In der Seitenleiste wird auch die Kategorie *Verbundene Geräte* angezeigt, die Informationen über die momentan am USB-Anschluss Ihres Computers angeschlossenen iPhone OS-Geräte enthält. Die Informationen über ein angeschlossenes Gerät werden automatisch zur Liste „Geräte" hinzugefügt und können angezeigt werden, ohne dass das Gerät erneut angeschlossen werden muss. Wenn ein Gerät angeschlossen ist, können Sie Profile, die ausschließlich auf dem angeschlossenen Gerät verwendet werden sollen, auch verschlüsseln.

Mit dem iPhone-Konfigurationsprogramm können Sie Konfigurationsprofile und Programme auf einem angeschlossenen Gerät installieren. Weitere Informationen finden Sie in den Abschnitten „Installieren von Konfigurationsprofilen mit dem iPhone-Konfigurationsprogramm" auf Seite 47, „Installieren von Programmen mithilfe des iPhone-Konfigurationsprogramms" auf Seite 76 und „Installieren von Vorlageprofilen mit dem iPhone-Konfigurationsprogramm" auf Seite 75.

Wenn ein Gerät angeschlossen ist, können Sie auch die Konsolenprotokolle und alle verfügbaren Protokolle über Systemfehler anzeigen. Dies sind die gleichen Geräteprotokolle, die auch innerhalb der Xcode-Entwicklungsumgebung unter Mac OS X verfügbar sind.

Erstellen von Konfigurationsprofilen

In diesem Dokument werden die Begriffe *Konfigurationsprofil* und *Payload-Segment* verwendet. Ein Konfigurationsprofil bezeichnet die gesamte Datei, mit der bestimmte (einzelne oder mehrere) Einstellungen auf dem iPhone, iPod touch oder iPad konfiguriert werden. Ein Payload-Segment bezeichnet eine Sammlung von Einstellungen eines bestimmten Typs (zum Beispiel die VPN-Einstellungen) innerhalb des Konfigurationsprofils.

Es ist zwar grundsätzlich möglich, ein einzelnes umfassendes Konfigurationsprofil zu erstellen, das alle für Ihre Organisation benötigten Payload-Segmente enthält. Sinnvoller ist es aber, ein Profil für Zertifikate und ein anderes Profil für einzelne oder mehrere andere Einstellungen zu verwenden, da Sie in diesem Fall die Möglichkeit haben, die Informationen jedes Typs einzeln zu aktualisieren und zu verteilen. Dadurch erhalten Benutzer die Möglichkeit, bereits installierte Zertifikate beizubehalten, wenn ein neues Profil installiert wird, das VPN- oder Account-Einstellungen enthält.

Bei vielen Payload-Segmenten können Sie Benutzernamen und Kennwörter eingeben. Wenn Sie diese Informationen weglassen, kann das Profil für mehrere Benutzer verwendet werden. Beim Installieren des Profils wird aber jeder Benutzer aufgefordert, die fehlenden Informationen einzugeben. Wenn Sie ein Profil für jeden Benutzer personalisieren und die zugehörigen Kennwörter integrieren, sollten Sie zum Schutz des Inhalts das Profil in verschlüsselter Form bereitstellen. Weitere Informationen finden im Abschnitt „Installieren von Konfigurationsprofilen" auf Seite 47.

Klicken Sie in der Symbolleiste des iPhone-Konfigurationsprogramms auf „Neu“, um ein neues Konfigurationsprofil zu erstellen. Danach können Sie mithilfe der Liste „Payloads“ dem Profil die gewünschten Payload-Segmente hinzufügen. Die hinzugefügten Payload-Segmente können Sie anschließend bearbeiten, indem Sie auswählen, welche der im Bearbeitungsbereich angebotenen Optionen verwendet werden sollen, bzw. die entsprechenden Informationen eingeben. Erforderliche Felder sind mit einem roten Pfeil markiert. Bei einigen Einstellungen (zum Beispiel den Wi-Fi-Einstellungen) können Sie auf die Taste „Hinzufügen“ (+) klicken, um Konfigurationen hinzuzufügen. Klicken Sie im Bearbeitungsbereich auf die Taste „Löschen“ (–), um eine Konfiguration zu löschen.

Wenn Sie ein Payload-Segment bearbeiten wollen, müssen Sie in der Liste „Payloads“ den entsprechenden Listeneintrag auswählen, auf „Konfigurieren“ klicken und wie nachfolgend beschrieben die erforderlichen Informationen eingeben.

Automatisieren der Erstellung von Konfigurationsprofilen

Sie können die Erstellung von Konfigurationsdateien auch mithilfe von AppleScript auf einem Mac oder C# Script unter Windows automatisieren. Führen Sie die folgenden Schritte aus, um die unterstützten Methoden und deren Syntax anzuzeigen:

- *Mac OS X:* Verwenden Sie den Skripteditor, um das AppleScript-Funktionsverzeichnis für das iPhone-Konfigurationsprogramm zu öffnen.
- *Windows*: Verwenden Sie Visual Studio, um die von iPCUScripting.dll bereitgestellten Methodenaufrufe anzuzeigen.

Verwenden Sie auf einem Mac den AppleScript-Befehl „Tell“, um ein Skript auszuführen. Übergeben Sie unter Windows den Skriptnamen als einen Befehlszeilen-Parameter an das iPhone-Konfigurationsprogramm.

Beispiele hierzu finden Sie unter Anhang C „Beispielskripte“

Einstellungen im Bereich „Allgemein“

In diesem Bereich können Sie den Namen und die Kennung für das Profil festlegen und angeben, ob Benutzer die Möglichkeit haben sollen, das Profil zu löschen, nachdem es installiert wurde.

Der Name, den Sie hier angeben, wird sowohl in der Profilliste als auch auf dem Gerät angezeigt (nachdem das Konfigurationsprofil installiert wurde). Der Name kann frei gewählt werden. Er muss nicht eindeutig sein, er sollte aber aussagekräftig sein und das Profil beschreiben.

Die Kennung muss das Profil eindeutig identifizieren und im Format com.*unternehmensname.kennung* eingegeben werden. Hierbei sollte eine Kurzbeschreibung des Profils als *Kennung* verwendet werden. (Beispiel: com.mycompany.homeoffice.)

Die Kennung ist wichtig, da bei der Installation des Profils dieser Wert mit den bereits auf dem Gerät installierten Profilen verglichen wird. Ist die Kennung eindeutig, werden die Informationen im Profil zum Gerät hinzugefügt. Stimmt die Kennung mit der Kennung eines bereits installierten Profils überein, werden die auf dem Gerät befindlichen Informationen durch die Einstellungen im Profil ersetzt. Ausgenommen davon sind nur die Exchange-Einstellungen. Zum Ändern eines Exchange-Accounts muss zunächst das Profil manuell entfernt werden, damit die zum Account gehörigen Daten gelöscht werden können.

Mit den Optionen im Einblendmenü „Sicherheit“ können Sie bestimmen, ob es Benutzern möglich sein soll, ein Profil nach der Installation zu löschen. Wenn Sie sich für die Option mit Autorisierung entscheiden, müssen Sie ein Kennwort festlegen, das beim Versuch, das Profil vom Gerät zu löschen, als Berechtigungsnachweis eingegeben werden muss. Wenn Sie die Option „Nie“ auswählen, kann das Profil mit einer neueren Version aktualisiert, nicht aber entfernt werden.

Einstellungen im Bereich „Code“

Mithilfe dieses Payload-Segments können Sie die Geräterichtlinien festlegen, sofern nicht die Coderichtlinien von Exchange verwendet werden sollen. Sie können festlegen, ob für die Verwendung des Geräts ein Code erforderlich ist, und darüber hinaus Charakteristika für den Code definieren und angeben, in welchen Zeitintervallen der Code geändert werden muss. Nach dem Laden des Konfigurationsprofils muss der Benutzer sofort einen Code eingeben, der den Richtlinien entspricht, die Sie auswählen. Geschieht dies nicht, wird das Profil nicht installiert.

Wenn Sie sowohl Geräterichtlinien als auch Exchange-Coderichtlinien verwenden, werden die beiden Richtliniengruppen kombiniert. In diesem Fall wird die jeweils strengere Einstellung verwendet. Informationen über unterstützte Exchange ActiveSync-Richtlinien finden Sie im Abschnitt „Microsoft Exchange ActiveSync“ auf Seite 9.

Folgende Richtlinien sind verfügbar:

- *Code-Eingabe auf Gerät erforderlich:* Der Benutzer muss auf dem Gerät einen Code eingeben, damit er das Gerät verwenden kann. Ist die Eingabe eines Codes nicht erforderlich, kann jeder, der im Besitz des Geräts ist, auf alle Funktionen und Daten zugreifen.
- *Einfache Werte erlauben:* Der Code darf aufeinander folgende oder sich wiederholende Zeichen enthalten. In diesem Fall sind beispielsweise Codes wie „3333“ oder „DEFG“ zulässig.
- *Alphanumerische Werte erforderlich:* Der Code muss mindestens ein alphabetisches Zeichen (Buchstaben) enthalten.
- *Mindestlänge des Codes:* Hier wird die Mindestanzahl der Zeichen für einen Code festgelegt.
- *Mindestanzahl von komplexen Zeichen:* Hier wird die Anzahl von nicht alphanumerischen Zeichen (wie $, & und !) festgelegt, die der Code enthalten muss.
- *Maximale Code-Gültigkeit (in Tagen):* Der Benutzer muss nach Ablauf des hier angegebenen Zeitintervalls den Code ändern.
- *Automatische Sperre (in Minuten):* Das Gerät wird automatisch gesperrt, wenn es für das hier angegebene Zeitintervall nicht verwendet wird. Durch Eingabe des Codes kann es wieder freigegeben werden.
- *Code-Verlauf:* Ein neuer Code wird abgewiesen, wenn er mit einem bereits zuvor verwendeten Code übereinstimmt. Sie können festlegen, wie viele frühere Codes für diesen Vergleich herangezogen werden sollen.
- *Zeitgrenze für Gerätesperrung:* Hier können Sie festlegen, in welchem zeitlichen Abstand nach der letzten Verwendung die Sperre des Geräts aufgehoben werden kann, ohne dass dafür der Code eingegeben werden muss.

- *Maximale Anzahl von Fehlversuchen:* Der hier ausgewählte Wert bestimmt die Anzahl der zulässigen Fehlversuche bei der Code-Eingabe, bevor alle Daten vom Gerät gelöscht werden. Wenn Sie diese Einstellung nicht ändern, erzwingt das Gerät nach sechs Fehlversuchen eine Zeitverzögerung. Erst nach Ablauf dieser Verzögerung ist ein neuer Versuch möglich, den Code einzugeben. Mit jedem Fehlversuch wird die Zeitverzögerung zum nächsten Versuch länger. Nach dem elften Fehlversuch, werden alle Daten und Einstellungen sicher vom Gerät gelöscht. Die Zeitverzögerung für die Code-Eingabe beginnt immer nach dem sechsten Fehlversuch. Wenn Sie also den Wert 6 oder einen niedrigeren Wert eingeben, gibt es keine Zeitverzögerung und das Gerät wird beim Erreichen der maximal zulässigen Eingabeversuche gelöscht.

Einstellungen im Bereich „Einschränkungen“

Mit diesem Payload-Segment legen Sie die Gerätefunktionen fest, die der Benutzer verwenden darf.

- *Anstößige Inhalte erlauben:* Wenn Sie diese Option ausschalten, werden im iTunes Store erworbene anstößige Musik- und Videotitel nicht angezeigt. Für Titel, die im iTunes Store angeboten werden, erfolgt gegebenenfalls die Kennzeichnung als „Anstößig“ durch den jeweiligen Inhalteanbieter (Content Provider).
- *Verwendung von Safari erlauben:* Wird diese Option ausgeschaltet, wird das Programm „Safari“ deaktiviert und sein Symbol aus dem Home-Bildschirm entfernt. Benutzer können in diesem Fall keine Webclips öffnen.
- *Verwendung von YouTube erlauben:* Wird diese Option ausgeschaltet, wird das Programm „YouTube“ deaktiviert und sein Symbol aus dem Home-Bildschirm entfernt.
- *Verwendung des iTunes Store erlauben:* Wird diese Option ausgeschaltet, wird das Programm „iTunes Store“ deaktiviert und sein Symbol aus dem Home-Bildschirm entfernt. Benutzer sind in diesem Fall nicht in der Lage, Inhalte in der Vorschau anzusehen, anzuhören, zu kaufen oder herunterzuladen.
- *Installation von Programmen erlauben:* Wird diese Option ausgeschaltet, wird der App Store deaktiviert und sein Symbol aus dem Home-Bildschirm entfernt. Benutzer können ihre Programme nicht installieren oder aktualisieren.
- *Verwendung der Kamera erlauben:* Wird diese Option ausgeschaltet, wird die Kamera vollständig deaktiviert und ihr Symbol aus dem Home-Bildschirm entfernt. Benutzer können in diesem Fall keine Fotos aufnehmen.
- *Bildschirmfoto erlauben:* Ist diese Option deaktiviert, können Benutzer kein Bildschirmfoto der Anzeige sichern.

Einstellungen im Bereich „Wi-Fi“

Mit diesem Payload-Segment wird festgelegt, wie das Gerät mit Ihrem drahtlosen Netzwerk verbunden wird. Durch Klicken auf die Taste „Hinzufügen“ (+) im Bearbeitungsbereich können Sie mehrere Netzwerkkonfigurationen erstellen und hinzufügen.

Der Benutzer kann nur eine Verbindung aufbauen, wenn diese Einstellungen festgelegt werden und den Anforderungen Ihres Netzwerks entsprechen.

- *Dienst-Set-Kennung (SSID, Service Set Identifier):* Hier wird die SSID des drahtlosen Netzwerks eingegeben, zu dem die Verbindung hergestellt werden soll.
- *Unsichtbares Netzwerk:* Hier wird angegeben, ob das Netzwerk seine Identität übermittelt.
- *Sicherheitstyp:* Wählen Sie eine Identifizierungsmethode für das Netzwerk aus. Die folgenden Auswahlmöglichkeiten stehen sowohl für private als auch für Unternehmensnetzwerke zur Verfügung.
  - *Ohne:* Das Netzwerk erfordert keine Identifizierung.
  - *WEP:* Das Netzwerk verwendet ausschließlich WEP-Identifizierung.
  - *WPA/WPA 2:* Das Netzwerk verwendet ausschließlich WPA-Identifizierung.
  - *Beliebig:* Das Gerät verwendet entweder die WEP- oder die WPA-Identifizierung, wenn es eine Verbindung zum Netzwerk herstellt. Es wird jedoch keine Verbindung zu nicht identifizierten Netzwerken hergestellt.
- *Kennwort:* Geben Sie das Kennwort für den Zugang zum drahtlosen Netzwerk ein. Wenn Sie dieses Feld leer lassen, wird der Benutzer aufgefordert, das Kennwort einzugeben.

Firmenweite Einstellungen

In diesem Abschnitt können Sie festlegen, wie das Gerät mit den Unternehmensnetzwerken verbunden wird. Diese Einstellungen werden angeboten, wenn Sie eine der Optionen für Firmen aus dem Einblendmenü „Sicherheitstyp“ auswählen.

Über „Protokolle“ können Sie festlegen, welche EAP-Verfahren für die Identifizierung und Konfiguration der EAP-FAST PACs (Protected Access Credential) verwendet werden sollen.

Über „Identifizierung“ können Sie Anmeldeeinstellungen wie einen Benutzernamen und die Identifizierungsprotokolle festlegen. Wenn Sie eine Identität über den Bereich „Zertifikate“ installiert haben, können Sie diese Identität aus dem Einblendmenü „Identitätszertifikat“ auswählen.

Über „Vertrauenswürdig“ können Sie angeben, welche Zertifikate bei der Überprüfung des Identifizierungsservers für die Wi-Fi-Verbindung als vertrauenswürdig eingestuft werden sollen. In der Liste der vertrauenswürdigen Zertifikate werden Zertifikate angezeigt, die über den Bereich „Zertifikate“ hinzugefügt wurden. Sie können in dieser Liste auswählen, welche Zertifikate als vertrauenswürdig betrachtet werden sollen. Fügen Sie die Namen der vertrauenswürdigen Identifizierungsserver zur Liste „Vertrauenswürdige Serverzertifikat-Namen“ hinzu. Sie können einen bestimmten Server angeben (wie *server.meinunternehmen.com*) oder einen Teilnamen (wie **.meinunternehmen.com*).

Mithilfe der Option „Ausnahmen erlauben“ können die Benutzer selbst entscheiden, ob ein Server als vertrauenswürdig eingestuft werden soll, wenn die Zertifikatshierarchie nicht hergestellt werden kann. Sollen keine Dialogfenster mit entsprechenden Aufforderungen angezeigt werden, und sollen nur Verbindungen zu vertrauenswürdigen Diensten hergestellt werden, sollte diese Option deaktiviert werden. Integrieren Sie in diesem Fall alle erforderlichen Zertifikate in das Profil.

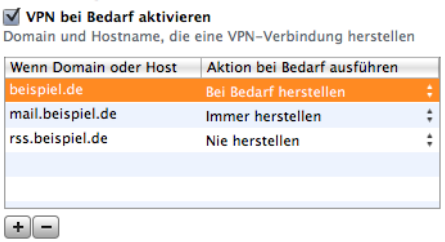
Einstellungen im Bereich „VPN“

Mit diesem Payload-Segment werden die VPN-Einstellungen für die Verbindung zu Ihrem Netzwerk festgelegt. Durch Klicken auf die Taste „Hinzufügen“ (+) können Sie mehrere Gruppen von VPN-Verbindungen hinzufügen.

Informationen über die unterstützten VPN-Protokolle und die Identifizierungsverfahren finden Sie im Abschnitt „VPN“ auf Seite 12. Welche Optionen im Einzelfall angeboten werden, hängt vom Protokoll und von der Art der Identifizierung ab, für die Sie sich entschieden haben.

VPN On Demand

Für zertifikatbasierte IPSec-Konfigurationen können Sie VPN bei Bedarf (On Demand) aktivieren, damit beim Zugriff auf bestimmte Domänen automatisch eine VPN-Verbindung hergestellt wird.



Für VPN On Demand werden die folgenden Einstellungen angeboten:

Einstellung	Beschreibung
Immer	Stellt eine VPN-Verbindung für eine beliebige Adresse her, die die angegebene Domäne umfassen.
Nie	Für Adressen, die die angegebene Domäne umfassen, wird keine VPN-Verbindung initiiert. Falls aber bereits eine VPN-Verbindung aktiv ist, kann sie genutzt werden.
Bei Bedarf herstellen	Für Adressen, die die angegebene Domäne umfassen, wird eine VPN-Verbindung nur hergestellt, wenn zuvor ein DNS-Lookup-Versuch fehlschlug.

Dieser Schritt gilt für alle entsprechenden Adressen. Adressen werden mithilfe eines einfachen Abgleichs von Zeichenfolgen verglichen (angefangen vom Ende in Rückwärtsrichtung). Die Adresse „.example.org“ entspricht den Domänen „support.example.org“ und „sales.example.org“, jedoch nicht „www.private-example.org“. Wenn Sie als Domäne jedoch „example.com“ angeben – ohne Punkt am Anfang – entspricht sie der Adresse „www.private-example.com“ und allen ähnlichen Adressen.

Beachten Sie, dass für LDAP-Verbindungen keine VPN-Verbindung initiiert wird. Wurde bereits durch ein anderes Programm (zum Beispiel durch Safari) eine VPN-Verbindung hergestellt, schlägt daher ein LDAP-Lookup-Vorgang fehl.

Einstellungen im Bereich „VPN“

Das iPhone unterstützt die manuelle VPN-Proxy-Konfiguration und auch die automatische Proxy-Konfiguration auf Basis von PAC oder WPAD. Wählen Sie eine der im Einblendmenü „Proxy-Konfiguration“ angebotenen Optionen aus, wenn Sie eine VPN-Proxy-Konfiguration definieren wollen.

Automatische Proxy-Konfiguration auf der Basis einer PAC-Datei – Wählen Sie „Automatisch“ aus dem Einblendmenü aus und geben Sie die URL einer PAC-Datei ein. Weitere Informationen über die Leistungsmerkmale und das Dateiformat von PACS finden Sie im Abschnitt „Weitere Informationsquellen“ auf Seite 64.

Automatische Proxy-Konfiguration auf der Basis von WPAD (Web Proxy Autodiscovery) – Wählen Sie „Automatisch“ aus dem Einblendmenü aus, lassen Sie aber das Feld „Proxy-Server-URL“ leer. In diesem Fall ruft das iPhone die WPAD-Datei mittels DHCP und DNS ab. Weitere Informationen über WPAD finden Sie unter „Weitere Informationsquellen“ auf Seite 64

Einstellungen im Bereich „E-Mail“

Mit diesem Payload-Segment werden die POP- bzw. IMAP-Mail-Accounts für den Benutzer definiert. Wenn Sie einen Exchange-Account hinzufügen, lesen Sie die Informationen unter „Einstellungen im Bereich „Exchange““ unten.

Die Benutzer können einige der E-Mail-Einstellungen ändern, die mit dem Profil bereitgestellt werden (wie etwa den Account-Namen, das Kennwort und alternative SMTP-Server). Wenn Sie eine dieser Informationen nicht im Profil definieren, werden die Benutzer aufgefordert, die entsprechenden Daten einzugeben, sobald sie sich beim Account anmelden.

Durch Klicken auf die Taste „Hinzufügen“ (+) können Sie mehrere E-Mail-Accounts hinzufügen.

Einstellungen im Bereich „Exchange“

Mit diesem Payload-Segment werden die Benutzereinstellungen für Ihren Exchange-Server festgelegt. Sie können ein Profil für einen spezifischen Benutzer erstellen, indem Sie den Benutzernamen, den Hostnamen und die E-Mail-Adresse angeben. Wenn Sie lediglich den Hostnamen angeben, werden die Benutzer aufgefordert, die übrigen Werte einzugeben, wenn sie das Profil installieren.

Wenn Sie im Profil den Benutzernamen, den Hostnamen und die SSL-Einstellungen festlegen, kann der Benutzer diese Einstellungen auf dem Gerät nicht ändern.

Sie können nur einen Exchange-Account pro Gerät konfigurieren. Andere E-Mail-Accounts (einschließlich Exchange-via-IMAP-Accounts) sind nicht betroffen, wenn Sie einen Exchange-Account hinzufügen. Exchange-Accounts, die mithilfe eines Profils hinzugefügt werden, werden automatisch gelöscht, wenn das Profil gelöscht wird. Auf andere Weise können sie nicht gelöscht werden.

Exchange synchronisiert standardmäßig die Kontakte, den Kalender und die E-Mail. Der Benutzer kann diese Einstellungen über „Einstellungen“ > „Accounts“ auf dem Gerät ändern (darunter auch wie viele Tage die Synchronisierung der Daten umfassen soll).

Wenn Sie die Option „SSL verwenden“ aktivieren, müssen Sie über den Bereich „Zertifikate“ die für die Identifizierung der Verbindung erforderlichen Zertifikate hinzufügen.

Klicken Sie auf „Hinzufügen“ (+), wenn Sie ein Zertifikat bereitstellen wollen, das den Benutzer gegenüber dem Exchange ActiveSync-Server identifiziert. Wählen Sie danach ein Identitätszertifikat aus dem Mac OS X-Programm „Schlüsselbundverwaltung“ oder dem Windows Certificate Store aus. Nachdem Sie ein Zertifikat hinzugefügt haben, können Sie den Authentication Credential Name eingeben, sofern diese Angabe für Ihre ActiveSync-Konfiguration erforderlich ist. Außerdem können Sie das Kennwort des Zertifikats in das Konfigurationsprofil einbetten. Wenn Sie das Kennwort nicht angeben, wird der Benutzer zu dessen Eingabe aufgefordert, wenn das Profil installiert wird.

Einstellungen im Bereich „LDAP“

Mit diesem Payload-Segment werden die Einstellungen für die Verbindung zu einem LDAPv3-Verzeichnis festgelegt. Mit der Taste „Hinzufügen“ (+) haben Sie die Möglichkeit, mehrere Suchbereiche für jedes Verzeichnis festzulegen und Verbindungen zu mehreren Verzeichnissen zu konfigurieren.

Wenn Sie die Option „SSL verwenden“ aktivieren, müssen Sie über den Bereich „Zertifikate“ die für die Identifizierung der Verbindung erforderlichen Zertifikate hinzufügen.

CalDAV-Einstellungen

Mit diesem Payload-Segment können Sie die Account-Einstellungen festlegen, die für die Verbindung zu einem CalDAV-konformen Kalenderserver benötigt werden. Diese Accounts werden zum Gerät hinzugefügt. Wie bei Exchange-Accounts müssen die Benutzer beim Installieren des Profils manuell die Informationen eingeben, die Sie im Profil nicht definiert haben (z. B. das Kennwort für den Account).

Wenn Sie die Option „SSL verwenden“ aktivieren, müssen Sie über den Bereich „Zertifikate“ die für die Identifizierung der Verbindung erforderlichen Zertifikate hinzufügen.

Durch Klicken auf die Taste „Hinzufügen“ (+) können Sie mehrere Accounts konfigurieren.

Einstellungen im Bereich „Abonnierte Kalender“

Mit diesem Payload-Segment können Sie dem Programm „Kalender“ auf dem Gerät Kalenderabonnements mit reinem Lesezugriff hinzufügen. Durch Klicken auf die Taste „Hinzufügen“ (+) können Sie mehrere Abonnements konfigurieren.

Eine Liste öffentlicher Kalender, die Sie abonnieren können, finden Sie auf der folgenden Website: www.apple.com/de/downloads/macosx/calendars/.

Wenn Sie die Option „SSL verwenden“ aktivieren, müssen Sie über den Bereich „Zertifikate“ die für die Identifizierung der Verbindung erforderlichen Zertifikate hinzufügen.

Einstellungen im Bereich „Webclip“

Mit diesem Payload-Segment können Sie dem Home-Bildschirm auf dem Gerät des Benutzers Webclips hinzufügen. Webclips ermöglichen den schnellen direkten Zugriff auf beliebte Webseiten.

Beachten Sie, dass die eingegebene URL das Präfix „http://“oder „https://“ umfasst. Ohne dieses Präfix funktioniert der Webclip nicht ordnungsgemäß. Möchten Siebeispielsweise die Online-Version des *iPhone-Benutzerhandbuchs* zum Home-Bildschirm hinzufügen, geben Sie die URL des Webclips an: http://help.apple.com/iphone/

Sie können ein eigenes Symbol für den Webclip hinzufügen. Wählen Sie dazu eine Grafikdatei im Format GIF, JPEG oder PNG und mit einer Größe von 59 x 60 Pixel aus. Das Bild wird automatisch entsprechend der Fenstergröße skaliert und beschnitten und falls erforderlich in das PNG-Format konvertiert.

Einstellungen im Bereich „Zertifikate“

Mit diesem Payload-Segment können Sie Zertifikate und Identitäten zum Gerät hinzufügen. Informationen zu unterstützten Formaten finden Sie unter „Zertifikate und Identitäten“ auf Seite 13.

Beim Installieren von Zertifikaten müssen auch die Intermediate-Zertifikate installiert werden, die auf dem Gerät zum Aufbau der Zertifikatskette zu einem vertrauenswürdigen Zertifikat benötigt werden. Eine Liste der bereits installierten Root-Zertifikate finden Sie im folgenden Apple Support-Artikel unter http://support.apple.com/kb/HT2185.

Wenn Sie eine Identität für die Nutzung mit Microsoft Exchange hinzufügen, verwenden Sie stattdessen das Payload-Segment „Exchange“. Beachten Sie hierzu die Informationen im Abschnitt „Einstellungen im Bereich „Exchange““ auf Seite 42.

Hinzufügen von Zertifikaten unter Mac OS X:

1. Klicken Sie auf die Taste „Hinzufügen“ (+).
2. Wählen Sie im nachfolgenden Dialogfenster eine PKCS1- oder eine PKSC12-Datei aus und klicken Sie auf „Öffnen“.

   Wenn Sie ein Zertifikat oder eine Identität installieren und dem Schlüsselbund hinzufügen wollen, können Sie es mit dem Programm „Schlüsselbundverwaltung“ in das Format „.p12“ exportieren. Das Programm „Schlüsselbundverwaltung“ befindet sich im Ordner „Programme“ > „Dienstprogramme“. Weitere Informationen finden Sie in der Online-Hilfe zum Programm „Schlüsselbundverwaltung“, die Sie über das Menü „Hilfe“ im geöffneten Programm anzeigen können.

   Klicken Sie erneut auf die Taste „Hinzufügen“ (+), wenn Sie dem Konfigurationsprofil weitere Zertifikate hinzufügen wollen.

Hinzufügen von Zertifikaten unter Windows:

1. Klicken Sie auf die Taste „Hinzufügen“ (+).
2. Wählen Sie aus dem Windows Certificate Store das Zertifikat aus, das Sie installieren wollen.

   Wenn das Zertifikat nicht in ihrem persönlichen Zertifikatedepot verfügbar ist, müssen Sie es zunächst hinzufügen und dessen privaten Schlüssel als „exportierbar“ markieren. Dieser Schritt wird vom Assistenten für den Import von Zertifikaten automatisch angeboten. Beachten Sie, dass Sie den administrativen Zugriff auf den Computer benötigen, wenn Sie ein Root-Zertifikat hinzufügen wollen, und dass das Zertifikat dem persönlichen Depot hinzugefügt werden muss.

Achten Sie darauf, dass keine Zertifikate dupliziert werden, wenn Sie mehrere Konfigurationsprofile verwenden. Es ist nicht möglich, mehrere Kopien desselben Zertifikats zu installieren.

Als Alternative zur Installation von Zertifikaten mithilfe eines Konfigurationsprofils können Sie festlegen, dass Benutzer die Zertifikate mithilfe von Safari von einer Webseite direkt auf ihre Geräte laden. Sie können die Zertifikate auch per E-Mail an die Benutzer senden. Weitere Informationen finden Sie im Abschnitt „Installieren von Identitäten und Root-Zertifikaten“ auf Seite 63. Mit den unten beschriebenen SCEP-Einstellungen können Sie festlegen, wie das Gerät beim Installieren des Profils die Zertifikate drahtlos abrufen kann.

Einstellungen im Bereich „SCEP“

Mit dem Payload-Segment „SCEP“ können Sie Einstellungen festlegen, die es dem Gerät ermöglichen, Zertifikate per SCEP (Simple Certificate Enrollment Protocol) von einer Zertifizierungsstelle (CA) zu beziehen.

Einstellung	Beschreibung
URL	Dies ist die Adresse des SCEP-Servers.
Name	Hierbei kann es sich um eine beliebige Zeichenkette handeln, die von der Zertifizierungsstelle erkannt und verstanden wird. Der Name kann beispielsweise zur Unterscheidung verschiedener Instanzen verwendet werden.
Betreff	Hierbei handelt es sich um die Darstellung eines X.500-Namens in Form eines Datenfelds aus OID und Wert. Beispiel: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar – Die übersetzte Form sieht wie folgt aus: [[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]]
Challenge	Hierbei handelt es sich um ein so genanntes Pre-Shared Secret, anhand dessen der SCEP-Server die Anforderung oder den Benutzer identifizieren kann.
Größe und Nutzung von Schlüsseln	Wählen Sie zunächst die Größe für den Schlüssel aus. Legen Sie danach mithilfe der Markierungsfelder die zulässige Verwendungsweise für den Schlüssel fest.
Fingerabdruck	Verwendet Ihre Zertifizierungsstelle HTTP, nutzen Sie dieses Feld, um den Fingerabdruck des Zertifikats der Zertifizierungsstelle bereitzustellen, mit dem das Gerät während der Registrierung die Authentizität der Antwort der Zertifizierungsstelle bestätigt. Sie können einen SHA1- oder MD5-Fingerabdruck eingeben oder ein Zertifikat für den Import der zugehörigen Signatur auswählen.

Weitere Informationen über den drahtlosen Abruf von Zertifikaten durch das iPhone finden Sie unter „Drahtlose Registrierung und Konfiguration“ auf Seite 25.

Einstellungen im Bereich „Erweitert“

Mit dem Payload-Segment „Erweitert“ können Sie den Zugangspunkt (Access Point Name, APN) des Geräts und die Proxy-Einstellungen für das Mobilfunknetz festlegen. Mit diesen Einstellungen wird definiert, wie das Gerät die Verbindung zum Netz des Netzbetreibers herstellt. Diese Einstellungen sollten Sie nur ändern, wenn Sie von einem Netzwerkexperten des Netzbetreibers dazu aufgefordert werden. Sind die Einstellungen falsch, kann das Gerät nicht über das Mobilfunknetz auf Daten zugreifen. Wurden versehentlich Änderungen an diesen Einstellungen vorgenommen, muss das entsprechende Profil vom Gerät gelöscht werden, um diese Änderungen rückgängig zu machen. Apple empfiehlt, APN-Einstellungen separat von anderen Unternehmenseinstellungen in einem eigenen Konfigurationsprofil zu definieren, da Profile mit APN-Informationen von Ihrem Mobilfunkanbieter signiert werden müssen.

Das iPhone OS unterstützt APN-Benutzernamen mit einer Länge von bis zu 20 Zeichen und Kennwörter mit bis zu 32 Zeichen.

Bearbeiten von Konfigurationsprofilen

Wählen Sie im iPhone-Konfigurationsprogramm ein Konfigurationsprofil aus. Verwenden Sie anschließend die Liste „Payloads“ und den Bearbeitungsbereich, um Änderungen vorzunehmen. Sie können außerdem auch ein Profil importieren, indem Sie „Ablage“ > „Zur Bibliothek hinzufügen“ auswählen und anschließend eine der .mobileconfig-Dateien auswählen. Wählen Sie „Ansicht“ > „Details einblenden“, wenn diese Einstellungen nicht angezeigt werden.

Das Gerät verwendet den Wert im Feld „Kennung“ des Payload-Segments „Allgemein“, um festzustellen, ob es sich um ein neues Profil oder um die Aktualisierung eines vorhandenen Profils handelt. Ändern Sie den Wert im Feld „Kennung“ nicht, wenn das aktualisierte Profil ein Profil ersetzen soll, das die Benutzer bereits installiert haben.

Installieren von Vorlageprofilen und Programmen

Mit dem iPhone-Konfigurationsprogramm können Sie Programme auf Geräten installieren, die an den Computer angeschlossen sind, und Vorlageprofile an diese Geräte verteilen. Weitere Informationen finden Sie in Kapitel 5 „Bereitstellen von Programmen“ auf Seite 73.

Installieren von Konfigurationsprofilen

Sie können ein von Ihnen erstelltes Profil mithilfe des iPhone-Konfigurationsprogramms auf einem angeschlossenen Gerät installieren.

Alternativ können Sie das Profil per E-Mail an die Benutzer senden oder es auf einer Website bereitstellen. Wenn die Benutzer auf ihrem Gerät die E-Mail öffnen oder das Profil von der Website laden, werden sie automatisch aufgefordert, die Installation zu starten.

Installieren von Konfigurationsprofilen mit dem iPhone-Konfigurationsprogramm

Mit dem iPhone-Konfigurationsprogramm können Sie Konfigurationsprofile direkt auf einem Gerät installieren, das auf iPhone OS 3.0 (oder neuer) aktualisiert wurde und an Ihren Computer angeschlossen ist. Sie können mit diesem Programm außerdem auch Profile entfernen, die zu einem früheren Zeitpunkt installiert wurden.

Ein Konfigurationsprofil installieren:

1. Schließen Sie das Gerät über ein USB-Kabel an Ihren Computer an.

   Das Gerät wird nach kurzer Wartezeit in der Geräteliste des iPhone-Konfigurationsprogramms angezeigt.
2. Wählen Sie das Gerät aus und öffnen Sie durch Klicken den Bereich „Konfigurationsprofile“.
3. Wählen Sie aus der Liste ein Konfigurationsprofil aus und klicken Sie auf „Installieren“.
4. Tippen Sie nun auf dem Gerät auf „Installieren“, um das ausgewählte Profil zu installieren.

   Wenn Sie ein Konfigurationsprofil über eine USB-Verbindung direkt auf einem Gerät installieren, wird es vor dem Transfer auf das Gerät automatisch verschlüsselt und signiert.

Verteilen der Konfigurationsprofile per E-Mail

Konfigurationsprofile können per E-Mail an Benutzer verteilt werden. Beim Eingang der E-Mail-Nachricht auf dem Gerät muss der jeweilige Benutzer lediglich auf den Anhang der E-Mail tippen, um die Installation des Profils zu starten.

Ein Konfigurationsprofil per E-Mail senden:

1. Klicken Sie in der Symbolleiste des iPhone-Konfigurationsprogramms auf das Symbol „Freigeben“.

Wählen Sie im nachfolgenden Dialogfenster eine der angebotenen Sicherheitsoptionen aus:

a *Ohne:* Eine .mobileconfig-Datei wird erstellt; hierbei handelt es sich um eine reine Textdatei. Sie kann auf jedem beliebigen Gerät installiert werden. Bestimmte Inhalte in der Datei werden unkenntlich gemacht, um dem Ausspionieren der Daten durch Unbefugte vorzubeugen.

b *Konfigurationsprofil signieren:* Die .mobileconfig-Datei wird signiert und wird von einem Gerät nicht installiert, wenn sie geändert wird. Bestimmte Felder werden unkenntlich gemacht, um dem Ausspionieren der Daten durch Unbefugte vorzubeugen. Nachdem das Profil installiert wurde, kann es nur durch ein Profil aktualisiert werden, das dieselbe Kennung aufweist und durch dieselbe Kopie des iPhone-Konfigurationsprogramms signiert wurde.

c *Profil signieren und verschlüsseln:*
Das Profil wird signiert, sodass es nicht geändert werden kann, und sein gesamter Inhalt wird verschlüsselt, damit er nicht durch Unbefugte gelesen werden kann. Außerdem kann das Profil nur einem bestimmten Gerät installiert werden. Diese Option wird für Profile empfohlen, die Kennwörter beinhalten. Für jedes Gerät, das Sie in der Geräteliste auswählen, wird eine separate .mobileconfig-Datei erstellt. Wenn ein Gerät nicht in der Liste angezeigt wird, so kann dies daran liegen, dass das Gerät bisher nie an den Computer angeschlossen wurde und der Verschlüsselungscode daher nicht abgerufen werden konnte oder dass das Gerät noch nicht auf iPhone OS 3.0 (oder neuer) aktualisiert wurde.

2 Klicken Sie auf „Freigeben“. Daraufhin wird im Programm „Mail“ (Mac OS X) bzw. „Outlook“ (Windows) eine neue Nachricht geöffnet, in die die definierten Profile als unkomprimierte Anhänge angefügt werden. Die Dateien müssen in unkomprimierter Form gesendet werden, damit das Gerät sie erkennt und das Profil installieren kann.

Verteilen der Konfigurationsprofile über das Web

Konfigurationsprofile können auf einer Website für Benutzer bereitgestellt werden. Benutzer können bereitgestellte Profile installieren, indem Sie sie mithilfe des Programms „Safari“ auf ihr Gerät laden. Die benötigte URL können Sie einfach per SMS an die Benutzer senden.

Ein Konfigurationsprofil exportieren:

1. Klicken Sie in der Symbolleiste des iPhone-Konfigurationsprogramms auf das Symbol „Exportieren“.

   Wählen Sie im nachfolgenden Dialogfenster eine der angebotenen Sicherheitsoptionen aus:

   a. *Ohne:* Eine .mobileconfig-Datei wird erstellt; hierbei handelt es sich um eine reine Textdatei. Sie kann auf jedem beliebigen Gerät installiert werden. Bestimmte Inhalte in der Datei werden unkenntlich gemacht, um dem Ausspionieren der Daten durch Unbefugte vorzubeugen. Sie sollten trotzdem aber darauf achten, dass die Website, auf der sie die Datei bereitstellen, nur für berechtigte Benutzer zugänglich ist.

   b. *Konfigurationsprofil signieren:* Die .mobileconfig-Datei wird signiert und wird von einem Gerät nicht installiert, wenn sie geändert wird. Nachdem das Profil installiert wurde, kann es nur durch ein Profil aktualisiert werden, das dieselbe Kennung aufweist und durch dieselbe Kopie des iPhone-Konfigurationsprogramms signiert wurde. Bestimmte Informationen im Profil werden unkenntlich gemacht, um dem Ausspionieren der Daten durch Unbefugte vorzubeugen. Sie sollten trotzdem aber darauf achten, dass die Website, auf der sie die Datei bereitstellen, nur für berechtigte Benutzer zugänglich ist.

   c. *Profil signieren und verschlüsseln:*
   Das Profil wird signiert, sodass es nicht geändert werden kann, und sein gesamter Inhalt wird verschlüsselt, damit er nicht durch Unbefugte gelesen werden kann. Außerdem kann das Profil nur einem bestimmten Gerät installiert werden. Für jedes Gerät, das Sie in der Geräteliste auswählen, wird eine separate .mobileconfig-Datei erstellt.

2. Klicken Sie auf „Exportieren“ und navigieren Sie zu dem Speicherort, an dem Sie die .mobileconfig-Dateien speichern wollen.

   Die Dateien können nun auf Ihrer Website bereitgestellt werden. Die .mobileconfig-Datei darf nicht komprimiert und ihre Erweiterung nicht geändert werden, da das Gerät die Datei sonst nicht erkennt und das Profil nicht installieren kann.

Benutzergesteuerte Installation geladener Konfigurationsprofile

Geben Sie den Benutzern die URL-Adresse bekannt, über die Profile auf die Geräte geladen werden können, oder senden Sie die Profile an einen E-Mail-Account, auf den die Benutzer mit dem Gerät zugreifen können, bevor das Gerät mit den unternehmensspezifischen Informationen konfiguriert wird.

Wenn ein Benutzer das Profil aus dem Web auf sein Gerät lädt oder im Programm „Mail“ den Anhang der E-Mail öffnet, erkennt das Gerät die Erweiterung „.mobileconfig“ als ein Profil und beginnt mit dessen Installation, sobald der Benutzer auf „Installieren“ tippt.

Während der Installation wird der Benutzer aufgefordert, alle Informationen einzugeben, die gemäß den von Ihnen festgelegten Einstellungen erforderlich sind (zum Beispiel im Profil nicht enthaltene Kennwörter).

Das Gerät ruft auch die Exchange ActiveSync-Richtlinien vom Server ab und aktualisiert die Richtlinien bei jedem nachfolgenden Verbindungsaufbau, falls sich diese zwischenzeitlich geändert haben. Falls das Gerät oder die Exchange ActiveSync-Richtlinien die Eingabe eines Gerätecodes vorschreiben, kann die Installation nur abgeschlossen werden, wenn der Benutzer einen Code eingibt, der der geltenden Richtlinie entspricht.

Darüber hinaus wird der Benutzer aufgefordert, die für die Verwendung der im Profil enthaltenen Zertifikate erforderlichen Kennwörter einzugeben.

Kann die Installation nicht erfolgreich abgeschlossen werden, da beispielsweise der Exchange-Server nicht verfügbar war oder der Benutzer den Installationsprozess abgebrochen hat, werden die bis zu diesem Zeitpunkt vom Benutzer eingegebenen Informationen nicht gespeichert.

Benutzer können individuell festlegen, die Nachrichten wie vieler Tage mit dem Gerät synchronisiert werden sollen und welche Mail-Ordner zusätzlich zum Posteingang synchronisiert werden sollen. Standardmäßig werden die Nachrichten der letzten drei Tage und alle Ordner synchronisiert. Benutzer können diese Einstellungen durch Auswahl von „Einstellungen“ > „Mail, Kontakte, Kalender“ > *Name des Exchange-Accounts* ändern.

Entfernen und Aktualisieren von Konfigurationsprofilen

Aktualisierte Konfigurationsprofile werden nicht sofort an die Benutzer weitergeleitet. Das bedeutet, dass Sie aktualisierte Profile an die Benutzer senden müssen, damit diese sie installieren können. Wenn die Kennungen des Profils auf dem Gerät und des aktualisierten Profils übereinstimmen und im Falle eines signierten Profils die Signierung durch dieselbe Kopie des iPhone-Konfigurationsprogramms erfolgte, wird das Profil auf dem Gerät durch das neue aktualisierte Profil ersetzt.

Einstellungen, die durch ein Konfigurationsprofil definiert sind, können auf dem Gerät nicht geändert werden. Soll eine Einstellung geändert werden, muss ein aktualisiertes Profil installiert werden. Ein signiertes Profil kann nur durch ein Profil ersetzt werden, das durch dieselbe Kopie des iPhone-Konfigurationsprogramms signiert wurde. Außerdem müssen das alte und das neue Profil dieselbe Kennung aufweisen, damit das Gerät das aktualisierte Profil als Ersatz für das vorhandene Profil erkennt. Weitere Informationen über die Kennung finden Sie im Abschnitt „Einstellungen im Bereich „Allgemein““ auf Seite 36.

Wichtig: Durch das Entfernen eines Konfigurationsprofils werden die Richtlinien und alle auf dem Gerät gespeicherten Daten des Exchange-Accounts sowie die VPN-Einstellungen, die Zertifikate und sonstige zum Profil gehörende Informationen (einschließlich aller E-Mail-Nachrichten) gelöscht.

Wenn im Payload-Segment „Allgemein“ des Profils festgelegt ist, dass der Benutzer das Profil nicht löschen kann, wird die Taste „Entfernen“ nicht angezeigt. Wenn im Profil ein Kennwort als Berechtigungsnachweis für das Löschen des Profils festgelegt wurde, wird der Benutzer zur Eingabe dieses Kennworts aufgefordert, wenn er auf „Entfernen“ tippt. Weitere Informationen über die Sicherheitseinstellungen für ein Profil finden Sie im Abschnitt „Einstellungen im Bereich „Allgemein““ auf Seite 36.

Manuelles Konfigurieren von Geräten

3

In diesem Kapitel wird beschrieben, wie Sie iPhone, iPod touch und iPad manuell konfigurieren.

Wenn Sie keine Profile für die automatische Konfiguration bereitstellen, können Benutzer ihre Geräte manuell konfigurieren. Einige Einstellungen wie Coderichtlinien können jedoch nur mit einem Konfigurationsprofil festgelegt werden.

VPN-Einstellungen

Zum Ändern von VPN-Einstellungen wählen Sie „Einstellungen" > „Allgemein" > „Netzwerk" > „VPN".

Wenn Sie VPN-Einstellungen konfigurieren, werden Sie zur Eingabe von Informationen aufgefordert. Welche Informationen das Gerät anfordert, hängt von den Antworten ab, die es von Ihrem VPN-Server erhält. So kann in Abhängigkeit vom Server beispielsweise ein RSA-SecurID-Token erforderlich sein.

Sie können eine zertifikatbasierte VPN-Verbindung erst dann konfigurieren, wenn die jeweiligen Zertifikate auf dem Gerät installiert sind. Weitere Informationen finden Sie im Abschnitt „Installieren von Identitäten und Root-Zertifikaten" auf Seite 63.

VPN On Demand kann nur mithilfe eines Konfigurationsprofils, nicht direkt auf dem Gerät konfiguriert werden. Vgl. „VPN On Demand" auf Seite 40.

VPN-Proxy-Einstellungen

Sie können VPN-Proxy-Einstellungen zusätzlich für alle Konfigurationen definieren. Wenn Sie für alle Verbindungen denselben Proxy-Server verwenden wollen, tippen Sie auf „Manuell“ und geben Sie die Adresse, den Port, den Benutzernamen und, sofern erforderlich, das Kennwort für die Anmeldung ein. Wenn Sie für das Gerät eine Datei für die automatische Proxy-Konfiguration verwenden wollen, müssen Sie auf „Auto(matisch)“ tippen und die URL der gewünschten PACS-Datei eingeben.
Für die automatische Proxy-Konfiguration per WPAD genügt es, wenn Sie nur auf „Auto(matisch)“ tippen, ohne eine URL einzugeben. Das Gerät ruft in diesem Fall die WPAD-Einstellungen über DHCP und DNS ab. Muster und Ressourcen für eine PACS-Datei finden Sie im Abschnitt „Weitere Informationsquellen“ am Ende dieses Kapitels.

Cisco-IPSec-Einstellungen

Wenn Sie das Gerät für eine Cisco-IPSec-VPN-Verbindung manuell konfigurieren, wird ein Bildschirm ähnlich dem folgenden angezeigt:

Der folgenden Tabelle können Sie entnehmen, welche Einstellungen und Informationen eingegeben werden müssen:

Feld	Beschreibung
Beschreibung	Ein beschreibender Titel, der diese Einstellungsgruppe identifiziert.
Server	Der DNS-Name oder die IP-Adresse des VPN-Servers, zu dem eine Verbindung hergestellt werden soll.
Account	Der Benutzername des VPN-Anmelde-Accounts des Benutzers. Geben Sie nicht den Gruppennamen in dieses Feld ein.
Kennwort	Das Kennwort des VPN-Anmelde-Accounts des Benutzers. Lassen Sie dieses Feld bei einer RSA-SecurID- und CryptoCard-Identifizierung leer. Gleiches gilt, wenn Benutzer ihr Kennwort bei jedem Verbindungsversuch manuell eingeben sollen.

Feld	Beschreibung
Zertifikat verwenden	Dieses Feld ist nur verfügbar, wenn Sie eine .p12- oder .pfx-Identität installiert haben, die ein für den Fernzugriff ausgelegtes Zertifikat *und* den privaten Schlüssel für das Zertifikat enthält. Ist das Feld „Zertifikat verwenden“ verfügbar, finden Sie anstelle der Felder „Gruppenname“ und „Shared Secret“ ein Feld zur Identifizierung, mit dem Sie eine installierte, mit VPN kompatible Identität auswählen können.
Gruppenname	Der Name der Gruppe, der der Benutzer angehört (wie auf dem VPN-Server definiert).
Shared Secret	Der Schlüssel („Shared Secret“) der Gruppe. Dieser Schlüssel ist für alle Mitglieder der zugewiesenen Gruppe des Benutzers identisch. Es handelt sich hierbei *nicht* um das Kennwort des Benutzers und der Schlüssel muss zum Aufbau einer Verbindung angegeben werden.

PPTP-Einstellungen

Wenn Sie das Gerät für eine PPTP-VPN-Verbindung manuell konfigurieren, wird ein Bildschirm ähnlich dem folgenden angezeigt:

Der folgenden Tabelle können Sie entnehmen, welche Einstellungen und Informationen eingegeben werden müssen:

Feld	Beschreibung
Beschreibung	Ein beschreibender Titel, der diese Einstellungsgruppe identifiziert.
Server	Der DNS-Name oder die IP-Adresse des VPN-Servers, zu dem eine Verbindung hergestellt werden soll.
Account	Der Benutzername des VPN-Anmelde-Accounts des Benutzers.
RSA-SecurID	Wenn Sie einen RSA-SecurID-Token verwenden, aktivieren Sie diese Option, damit das Feld „Kennwort“ ausgeblendet wird.

Feld	Beschreibung
Kennwort	Das Kennwort des VPN-Anmelde-Accounts des Benutzers.
Verschlüsselungsgrad	Die Standardeinstellung ist „Auto“. Damit wird die höchste verfügbare Verschlüsselungsstufe gewählt. (Die Stufen sind 128 Bit, 40 Bit oder keine Verschlüsselung.) Die höchste verfügbare Stufe ist 128 Bit. Mit der Einstellung „Keiner“ wird die Verschlüsselung deaktiviert.
Für alle Daten	Der Standardwert ist „Ein“. Damit wird der gesamte Netzwerkverkehr über die VPN-Verbindung übertragen. Deaktivieren Sie diese Option, um das Split-Tunneling (geteiltes Tunneling) zu aktivieren, bei dem nur die Daten, die an Server innerhalb des VPN übertragen werden sollen, über die VPN-Verbindung geleitet werden. Der übrige Datenverkehr wird über das Internet gesendet.

L2TP-Einstellungen

Wenn Sie das Gerät für eine L2TP-VPN-Verbindung manuell konfigurieren, wird ein Bildschirm ähnlich dem folgenden angezeigt:

Der folgenden Tabelle können Sie entnehmen, welche Einstellungen und Informationen eingegeben werden müssen:

Feld	Beschreibung
Beschreibung	Ein beschreibender Titel, der diese Einstellungsgruppe identifiziert.
Server	Der DNS-Name oder die IP-Adresse des VPN-Servers, zu dem eine Verbindung hergestellt werden soll.
Account	Der Benutzername des VPN-Anmelde-Accounts des Benutzers.
Kennwort	Das Kennwort des VPN-Anmelde-Accounts des Benutzers.

Feld	Beschreibung
Shared Secret	Der Pre-Shared-Schlüssel („Shared Secret“) für den L2TP-Account. Dieser Schlüssel ist für alle LT2P-Benutzer identisch.
Für alle Daten	Der Standardwert ist „Ein“. Damit wird der gesamte Netzwerkverkehr über die VPN-Verbindung übertragen. Deaktivieren Sie diese Option, um das Split-Tunneling (geteiltes Tunneling) zu aktivieren, bei dem nur die Daten, die an Server innerhalb des VPN übertragen werden sollen, über die VPN-Verbindung geleitet werden. Der übrige Datenverkehr wird über das Internet gesendet.

Wi-Fi-Einstellungen

Zum Ändern von Wi-Fi-Einstellungen wählen Sie „Einstellungen“ > „Allgemein“ > „Netzwerk“ > „Wi-Fi“. Befindet sich das Netzwerk, das Sie hinzufügen, in Reichweite, wählen Sie es aus der Liste der verfügbaren Netzwerke aus. Andernfalls tippen Sie auf „Anderes“.

Vergewissern Sie sich, dass Ihre Netzwerkinfrastruktur eine vom iPhone und iPod touch unterstützte Identifizierung und Verschlüsselung verwendet. Nähere Angaben hierzu finden Sie im Abschnitt „Netzwerksicherheit“ auf Seite 12. Weitere Informationen zum Installieren von Zertifikaten für die Identifizierung finden Sie im Abschnitt „Installieren von Identitäten und Root-Zertifikaten“ auf Seite 63.

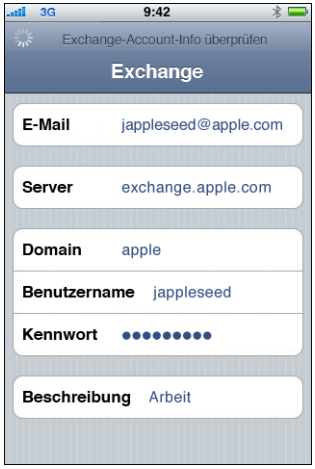
Exchange-Einstellungen

Sie können nur einen Exchange-Account pro Gerät konfigurieren. Wenn Sie einen Exchange-Account hinzufügen möchten, wählen Sie „Einstellungen“ > „Mail, Kontakte, Kalender“ und tippen dann auf „Account hinzufügen“. Tippen Sie im Bildschirm „Account hinzufügen“ auf „Microsoft Exchange“.

Wenn Sie das Gerät manuell für Exchange konfigurieren, können Sie der folgenden Tabelle entnehmen, welche Einstellungen und Informationen erforderlich sind:

Feld	Beschreibung
E-Mail	Die vollständige E-Mail-Adresse des Benutzers.
Domain	Die Domain des Exchange-Accounts des Benutzers.
Benutzername	Der Benutzername des Exchange-Accounts des Benutzers.
Kennwort	Das Kennwort des Exchange-Accounts des Benutzers.
Beschreibung	Eine Kurzbeschreibung zur Identifizierung dieses Accounts.

iPhone, iPod touch und iPad unterstützen den Autodiscover-Dienst von Microsoft, der anhand Ihres Benutzernamens und Kennworts die Adresse des Frontend-Exchange-Servers ermittelt. Kann die Adresse des Servers nicht ermittelt werden, werden Sie aufgefordert, sie einzugeben.



Wenn Ihr Exchange-Server einen anderen Port als 443 auf Verbindungen abhört, geben Sie die entsprechende Portnummer im folgenden Format in das Feld „Server“ ein: *exchange.beispiel.com:portnummer*.

Nachdem der Exchange-Account erfolgreich konfiguriert wurde, werden die Kennwortrichtlinien des Servers umgesetzt. Wenn der aktuelle Code des Benutzers die Exchange ActiveSync-Richtlinien nicht erfüllt, wird der Benutzer aufgefordert, den Code zu ändern oder entsprechend festzulegen. Das Gerät kann erst mit dem Exchange-Server kommunizieren, nachdem der Benutzer einen passenden Code festgelegt hat.

Anschließend bietet das Gerät eine Option zur sofortigen Synchronisierung mit dem Exchange-Server an. Wenn Sie die Synchronisierung zu einem späteren Zeitpunkt ausführen möchten, können Sie Kalender und Kontakte später durch Auswahl von „Einstellungen" > „Mail, Kontakte, Kalender" synchronisieren. Exchange ActiveSync überträgt neue, auf Ihrem Server eingehende Daten standardmäßig via Push-Funktion auf Ihr Gerät. Wählen Sie „Einstellungen" > „Mail, Kontakte, Kalender" > „Neue Daten laden" aus, wenn Sie diese Einstellung ändern und neue Daten lieber manuell in festgelegten Zeitabständen bzw. nur neue Daten abrufen wollen.

Wenn Sie „Einstellungen" > „Mail, Kontakte, Kalender" und anschließend den Exchange-Account auswählen, können Sie den Zeitraum (als Anzahl von Tagen) angeben, für den Mail-Nachrichten mit Ihrem Gerät synchronisiert werden sollen. Außerdem können Sie festlegen, welche Ordner zusätzlich zum Posteingang in die Mail-Zustellung mittels Push-Funktion eingebunden werden sollen.

Durch Auswahl von „Einstellungen" > „Mail, Kontakte, Kalender" > „Sync" können Sie die Einstellung für Kalenderdaten ändern.

Einstellungen im Bereich „LDAP“

iPhone, iPod touch und iPad können Kontaktinformationen von LDAP-Verzeichnisservern abrufen. Wählen Sie „Einstellungen“ > „Mail, Kontakte, Kalender“ und tippen Sie auf „Account hinzufügen“, wenn Sie einen LDAP-Server hinzufügen wollen. Tippen Sie anschließend auf „LDAP-Account hinzufügen“.

Geben Sie die Adresse des LDAP-Servers, den Benutzernamen und, sofern erforderlich, das zugehörige Kennwort ein und tippen Sie auf „Weiter“. Wenn der Server zugänglich ist und Standardsucheinstellungen für das Gerät bereitstellt, werden diese Einstellungen verwendet.

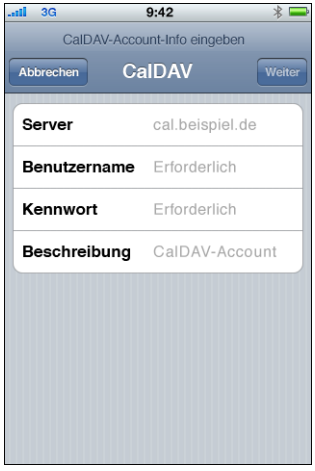
Für die Option „Suchmodus“ werden die folgenden Einstellungen unterstützt:

Einstellung für „Suchmodus“	Beschreibung
Suchbereich	Nur das Basisobjekt wird durchsucht.
Eine Ebene	Nur die Objekte der Ebene unmittelbar unterhalb des Basisobjekts werden durchsucht. Das Basisobjekt selbst wird nicht durchsucht.
Teilbaum	Zusätzlich zum Basisobjekt wird die gesamte Struktur aller vom Basisobjekt ausgehenden Objekte durchsucht.

Für jeden Server können mehrere Gruppen mit Sucheinstellungen definiert werden.

CalDAV-Einstellungen

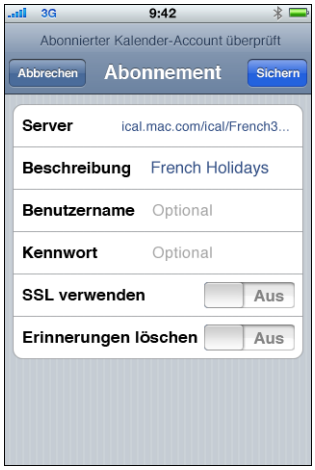
Für die Arbeit mit Gruppenkalendern und die gemeinsame Zeitplanung kommunizieren iPhone, iPod touch und iPad mit CalDAV-Kalenderservern. Wählen Sie „Einstellungen“ > „Mail, Kontakte, Kalender“ und tippen Sie auf „Account hinzufügen“, wenn Sie einen CalDAV-Server hinzufügen wollen. Tippen Sie anschließend auf „CalDAV-Account hinzufügen“.



Geben Sie die Adresse des CalDAV-Servers, den Benutzernamen und, sofern erforderlich, das zugehörige Kennwort ein und tippen Sie auf „Weiter“. Nachdem der Kontakt zum Server hergestellt wurde, werden weitere Felder angezeigt, mit denen Sie zusätzliche Optionen einrichten können.

Einstellungen für Kalenderabonnements

Sie können im Lesezugriff bereitgestellte Kalender hinzufügen (zum Beispiele für Projektzeitpläne und die Urlaubsplanung). Wählen Sie zum Hinzufügen eines Kalenders „Einstellungen“ > „Mail, Kontakte, Kalender“ > „Account hinzufügen“ > „Weitere“ und tippen Sie auf „Abonnierten Kalender hinzufügen“.



Geben Sie die URL für eine iCalendar-Datei (.ics), den Benutzernamen und, sofern erforderlich, das zugehörige Kennwort ein und tippen Sie auf „Sichern“. Wenn Sie dem Gerät einen Kalender hinzufügen, können Sie angeben, ob im Kalender definierte Erinnerungen entfernt oder beibehalten werden sollen.

Ein abonnierter Kalender kann nicht nur auf die oben beschriebene Weise manuell hinzugefügt werden. Sie können einem Benutzer alternativ auch den Link zu einer .ics-Datei im Format „webcal:// URL“ (oder „http://“) senden. Tippt der Benutzer auf diesen Link, bietet ihm das Gerät an, den abonnierten Kalender hinzuzufügen.

Installieren von Identitäten und Root-Zertifikaten

Wenn Sie Zertifikate nicht mithilfe von Profilen weitergeben, können Ihre Benutzer sie manuell installieren. Dazu laden sie die Zertifikate entweder mit ihrem Gerät von einer Website oder öffnen einen Anhang in einer E-Mail. Das Gerät erkennt Zertifikate mit den folgenden MIME-Typen und Dateierweiterungen:

- application/x-pkcs12, .p12, .pfx
- application/x-x509-ca-cert, .cer, .crt, .der

Im Abschnitt „Zertifikate und Identitäten“ auf Seite 13 finden Sie weitere Informationen zu den unterstützten Formaten und zu den zusätzlichen Anforderungen.

Wird ein Zertifikat oder eine Identität auf das Gerät geladen, wird der Bildschirm „Profil installieren“ angezeigt. Die Beschreibung gibt Aufschluss über den Typ: Identität bzw. CA (Certificate Authority). Tippen Sie auf „Installieren“, um das Zertifikat zu installieren. Im Falle eines Identitätszertifikats werden Sie aufgefordert, zusätzlich das Kennwort für das Zertifikat einzugeben.

Wählen Sie „Einstellungen“ > „Allgemein“ > „Profil“, wenn Sie ein installiertes Zertifikat anzeigen oder entfernen wollen. Wenn Sie ein Zertifikat entfernen, das für den Zugriff auf einen Account oder ein Netzwerk erforderlich ist, kann Ihr Gerät nicht mehr auf die betreffenden Dienste zugreifen.

Zusätzliche Mail-Accounts

Sie können zwar nur einen Exchange-Account konfigurieren, aber mehrere POP- und IMAP-Accounts hinzufügen. Damit wird beispielsweise der Zugriff auf E-Mails auf einem Lotus Notes- oder Novell Groupwise-Mail-Server möglich. Wählen Sie „Einstellungen" > „Accounts" > „Mail, Kontakte, Kalender" > „Account hinzufügen" > „Weitere" aus. Weitere Informationen zum Hinzufügen eines IMAP-Accounts finden Sie im *iPhone-Benutzerhandbuch, iPod touch-Benutzerhandbuch* oder im *iPad-Benutzerhandbuch*.

Entfernen und Aktualisieren von Profilen

Weitere Informationen über das Aktualisieren und Entfernen von Konfigurationsprofilen durch den Benutzer finden Sie im Abschnitt „Entfernen und Aktualisieren von Konfigurationsprofilen" auf Seite 51.

Weitere Informationen über das Installieren von Vorlageprofilen für das Verteilen und Senden finden Sie im Abschnitt „Bereitstellen von Programmen" auf Seite 73.

Weitere Informationsquellen

Weitere Informationen über das Format und die Funktionsweise von Dateien für die automatische Proxy-Konfiguration, die für die VPN-Proxy-Einstellungen verwendet werden, finden Sie an den folgenden Orten:

- Proxy Auto-Config (PAC) unter der Adresse: http://de.wikipedia.org/wiki/Proxy_Auto-Config
- Web Proxy Autodiscovery Protocol unter der Adresse: http://de.wikipedia.org/wiki/WPAD
- Microsoft TechNet „Using Automatic Configuration, Automatic Proxy, and Automatic Detection" unter http://technet.microsoft.com/en-us/library/dd361918.aspx

Apple stellt mehrere, in einem standardmäßigen Webbrowser anzeigbare Videoeinführungen für Ihre Benutzer bereit, in denen erläutert wird, wie die Funktionen von iPhone, iPod touch und iPad eingerichtet und verwendet werden:

- iPhone-Videotour unter der Adresse: www.apple.com/de/iphone/guidedtour/
- iPod touch-Videotour unter der Adresse: www.apple.com/de/ipodtouch/guidedtour/
- iPad-Videotour unter der Adresse: www.apple.com/ipad/guided-tours/
- iPhone-Support-Webseite unter der Adresse: www.apple.com/de/support/iphone/
- iPod touch-Support-Webseite unter der Adresse: www.apple.com/de/support/ipodtouch/
- iPad-Support-Webseite unter der Adresse: www.apple.com/de/support/ipad/

Zu jedem Gerät ist auch ein Benutzerhandbuch als PDF-Datei verfügbar, das zusätzliche Tipps und Details zur Verwendung umfasst:

- *iPhone-Benutzerhandbuch:*
  http://manuals.info.apple.com/de_DE/iPhone_Benutzerhandbuch.pdf
- *iPod touch-Benutzerhandbuch:*
  http://manuals.info.apple.com/de_DE/iPod_touch_2.0_Benutzerhandbuch.pdf
- *iPad-Benutzerhandbuch*:
  http://manuals.info.apple.com/de_DE/iPad_Benutzerhandbuch.pdf

Bereitstellen von iTunes

4

Sie verwenden iTunes, um Musik und Videos zu synchronisieren, Programme zu installieren und mehr.

In diesem Kapitel wird beschrieben, wie Sie iTunes und unternehmenseigene Programme bereitstellen. Außerdem werden die Einstellungen und Einschränkungen genannt, die Sie festlegen können.

iPhone, iPod touch und iPad können Daten eines bestimmten Typs (Musik, Medien usw.) immer nur mit jeweils einem Computer synchronisieren. Sie können beispielsweise Ihre Musiktitel mit einem Desktop-Computer und Ihre Lesezeichen mit einem mobilen Computer synchronisieren, sofern die Synchronisationsoptionen im Programm „iTunes" auf den beiden Computern entsprechend konfiguriert sind. Weitere Informationen über die Synchronisationsoptionen finden Sie in der Online-Hilfe zum Programm „iTunes", auf die Sie im geöffneten Programm über das Menü „Hilfe" zugreifen können.

Installieren von iTunes

iTunes verwendet standardmäßige Macintosh- und Windows-Installationsprogramme. Die jeweils neueste Version sowie eine Übersicht über die Systemanforderungen stehen auf der Website „www.itunes.com/de" als Downloads zur Verfügung.

Weitere Informationen über die Lizenzbestimmungen für die Verteilung des Programms „iTunes" finden Sie auf der folgenden Website:
http://developer.apple.com/softwarelicensing/agreements/itunes.html

Installieren von iTunes auf Windows-Computern

Wenn Sie iTunes auf Windows-Computern installieren, werden standardmäßig auch die aktuellsten Versionen von QuickTime, Bonjour und Apple Software Update installiert. Sie können diese Komponenten auslassen, indem Sie die Einstellungen im iTunes-Installationsprogramm entsprechend festlegen oder indem Sie nur die zu installierenden Komponenten auf die Computer Ihrer Benutzer übertragen.

Installieren unter Windows mit der Datei „iTunesSetup.exe“

Wenn Sie beabsichtigen, den standardmäßigen iTunes-Installationsprozess zu verwenden, jedoch einige Komponenten weglassen möchten, können Sie über die Eingabeaufforderung Attribute für die Datei „iTunesSetup.exe“ festlegen.

Attribut	Bedeutung
NO_AMDS=1	Apple Mobile Device Services (AMDS) wird nicht installiert. Diese Komponente ist für die Synchronisierung und Verwaltung mobiler Geräte in iTunes erforderlich.
NO_ASUW=1	Apple Software Update für Windows (ASUW) wird nicht installiert. Mit diesem Programm werden Benutzer auf neue Versionen von Apple-Software aufmerksam gemacht.
NO_BONJOUR=1	Bonjour wird nicht installiert. Bonjour ermöglicht eine Ankündigung von Druckern, freigegebenen iTunes-Mediatheken und anderen Diensten im Netzwerk ohne vorhergehende Konfiguration.
NO_QUICKTIME=1	QuickTime wird nicht installiert. Diese Komponente ist für die Verwendung von iTunes erforderlich. Lassen Sie QuickTime nicht weg, es sei denn, Sie sind sich sicher, dass auf dem Client-Computer bereits die aktuellste Version installiert ist.

Installation unter Windows ohne Benutzereingriff

Wenn Sie iTunes ohne Benutzereingriff installieren wollen, müssen Sie die einzelnen .msi-Dateien aus der Paketdatei „iTunesSetup.exe“ extrahieren und sie mithilfe der Push-Funktion auf die Client-Computer übertragen.

.msi-Dateien aus der Paketdatei „iTunesSetup.exe“ extrahieren:

1. Führen Sie die Datei „iTunesSetup.exe“ aus.
2. Öffnen Sie den Ordner „*%temp%*“ und suchen Sie darin nach dem Ordner „IXP*nnn*.TMP“. „*%temp%*“ steht dabei für Ihr temporäres Verzeichnis und „*nnn*“ für eine aus drei Ziffern bestehende Zufallszahl. Unter Windows XP handelt es sich bei diesem temporären Verzeichnis normalerweise um das Verzeichnis „*Startlaufwerk*:\Dokumente und Einstellungen*benutzername*\Lokale Einstellungen\Temp\“. Unter Windows Vista handelt es sich bei diesem temporären Verzeichnis normalerweise um das Verzeichnis „\Benutzer*benutzername*\AppData\Local\Temp\“.
3. Kopieren Sie die .msi-Dateien aus dem Ordner an einen anderen Speicherort.
4. Beenden Sie das Installationsprogramm, das von iTunesSetup.exe geöffnet wurde.

Verwenden Sie dann den Gruppenrichtlinienobjekt-Editor der Microsoft Verwaltungskonsole, um die .msi-Dateien zu einer Richtlinie für die Computerkonfiguration hinzuzufügen. Vergewissern Sie sich, dass Sie die Konfiguration zur Richtlinie für die Computerkonfiguration und nicht zur Richtlinie für die Benutzerkonfiguration hinzufügen.

Wichtig: iTunes erfordert QuickTime und Apple Application Support. Apple Application Support muss vor iTunes installiert werden. Apple Mobile Device Services (AMDS) wird benötigt, um ein iPhone, einen iPod touch oder ein iPad mit iTunes zu verwenden.

Bevor Sie die .msi-Dateien mittels Push-Funktion transferieren, müssen Sie angeben, in welchen lokalisierten Versionen das Programm „iTunes" installiert werden soll. Öffnen Sie dazu die .msi-Datei mit dem Werkzeug „ORCA", das mit der Windows SDK-Software als Datei „Orca.msi" im Verzeichnis „bin\" installiert wird. Bearbeiten Sie mit diesem Werkzeug die Angaben im Bereich „Summary Information Stream" und entfernen Sie die Namen der Sprachen, in denen das Programm nicht installiert werden soll. (Die Locale-Angabe „ID1033" steht für „Englisch".) Alternativ können Sie mit dem Editor für Gruppenrichtlinien in den Eigenschaften der .msi-Dateien für die Verteilung die Option „Sprache ignorieren" einstellen.

Installieren von iTunes auf Mac-Computern

Auf Mac-Computern ist iTunes bereits installiert. Die jeweils neueste Version von iTunes steht auf der Website „www.itunes.com/de" als Download zur Verfügung. Für die Übertragung von iTunes auf Mac-Clients können Sie das Programm „Arbeitsgruppenmanager" von Mac OS X Server verwenden.

Schnelles Aktivieren von Geräten mit iTunes

Bevor ein neues Gerät (iPhone, iPod touch oder iPad) verwendet werden kann, muss das Gerät aktiviert werden. Hierfür muss das Gerät an einen Computer angeschlossen werden, auf dem iTunes ausgeführt wird. Normalerweise werden Sie von iTunes nach dem Aktivieren eines Geräts gefragt, ob das Gerät mit dem Computer synchronisiert werden soll. Damit dies vermieden wird, wenn Sie für jemanden anderen ein Gerät konfigurieren, sollten Sie den reinen Aktivierungsmodus verwenden. In diesem Fall wirft iTunes das Gerät automatisch aus, nachdem es aktiviert wurde. Anschließend kann das Gerät konfiguriert werden, ohne dass sich Medien oder Daten auf dem Gerät befinden.

Den reinen Aktivierungsmodus unter Mac OS X verwenden:

1. Vergewissern Sie sich, dass iTunes nicht ausgeführt wird, und öffnen Sie das Programm „Terminal".
2. Geben Sie in Terminal einen der folgenden Befehle ein:
   - Verwenden des reinen Aktivierungsmodus:
     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 1
     ```
   - Deaktivieren des reinen Aktivierungsmodus:
     ```
     defaults delete com.apple.iTunes StoreActivationMode
     ```

Das Aktivieren eines Geräts ist im Abschnitt „Verwenden des reinen Aktivierungsmodus" beschrieben.

Den reinen Aktivierungsmodus unter Windows verwenden:

1. Vergewissern Sie sich, dass iTunes nicht ausgeführt wird, und öffnen Sie ein Eingabeaufforderungsfenster.
2. Geben Sie einen der folgenden Befehle ein:
   - Verwenden des reinen Aktivierungsmodus:

     ```
     "C:\Programme\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 1
     ```
   - Deaktivieren des reinen Aktivierungsmodus:

     ```
     "C:\Programme\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 0
     ```

   Sie können auch eine Verknüpfung erstellen oder die bereits vorhandene iTunes-Verknüpfung bearbeiten und diese Befehle integrieren, damit schnell zwischen den Aktivierungsmodi gewechselt werden kann.

Sie können feststellen, ob der reine Aktivierungsmodus aktiviert ist, indem Sie „iTunes" > „Über iTunes" auswählen und überprüfen, ob unter den Versions- und Build-Informationen für iTunes die Angabe „Reiner Aktivierungsmodus" angezeigt wird.

Verwenden des reinen Aktivierungsmodus

Stellen Sie sicher, dass der reine Aktivierungsmodus wie oben beschrieben aktiviert wurde, und führen Sie anschließend die folgenden Schritte aus.

1. Wenn Sie ein iPhone aktivieren möchten, legen Sie eine aktivierte SIM-Karte ein. Verwenden Sie das Werkzeug zum Auswerfen der SIM-Karte bzw. eine aufgebogene Büroklammer, um das SIM-Fach zu öffnen. Im *iPhone-Benutzerhandbuch* finden Sie weitere Informationen.
2. Schließen Sie iPhone, iPod touch oder iPad an den Computer an. Der Computer muss mit dem Internet verbunden sein, damit die Aktivierung des Geräts ausgeführt werden kann.

   iTunes wird ggf. geöffnet und aktiviert das Gerät. Sobald das Gerät erfolgreich aktiviert wurde, wird eine entsprechende Nachricht angezeigt.
3. Trennen Sie das Gerät vom Computer.

   Sie können sofort weitere Geräte anschließen und aktivieren. Solange der reine Aktivierungsmodus verwendet wird, synchronisiert iTunes die Geräte nicht. Soll iTunes die Synchronisation mit den Geräten wieder aufnehmen, muss der reine Aktivierungsmodus deaktiviert werden.

Festlegen von iTunes-Einschränkungen

Sie können festlegen, dass Ihre Benutzer bestimmte iTunes-Funktionen nicht verwenden dürfen. Diese Funktion wird auch als „Kindersicherung" bezeichnet. Der Zugriff auf folgende Funktionen kann eingeschränkt werden:

- Automatisches und vom Benutzer gestartetes Überprüfen auf neue iTunes-Versionen und Softwareaktualisierungen für Geräte

- Anzeigen von Genius-Vorschlägen beim Durchsuchen und Wiedergeben von Medien
- Automatisches Synchronisieren beim Anschließen von Geräten
- Laden von CD-Covern
- Verwenden von Plug-Ins für visuelle Effekte
- Eingeben einer URL-Adresse von Streaming-Medien
- Automatisches Erkennen von Apple TV-Systemen
- Registrieren neuer Geräte bei Apple
- Abonnieren von Podcasts
- Wiedergeben von Internetradio
- Zugreifen auf den iTunes Store
- Gemeinsame Nutzung der Mediathek mit anderen Computern im lokalen Netzwerk, auf denen iTunes installiert ist
- Abspielen von iTunes-Inhalten, die als anstößig gekennzeichnet sind
- Abspielen von Filmen
- Abspielen von TV-Sendungen

Festlegen von iTunes-Einschränkungen für Mac OS X

Unter Mac OS X steuern Sie den Zugriff durch die Verwendung bestimmter Schlüssel in einer plist-Datei. Die genannten Schlüsselwerte können unter Mac OS X für alle Benutzer festgelegt werden, indem Sie die Datei „~/Library/Preferences/com.apple.iTunes.plist“ mit dem Programm „Arbeitsgruppenmanager“ bearbeiten, das Bestandteil von Mac OS X Server ist.

Anleitungen hierzu finden Sie im Apple-Support-Artikel unter der Adresse: http://docs.info.apple.com/article.html?artnum=303099.

Festlegen von iTunes-Einschränkungen für Windows

Unter Windows steuern Sie den Zugriff, indem Sie Registrierungswerte in einem der folgenden Registrierungsschlüssel festlegen:

Unter Windows XP und Windows Vista mit 32 Bit:

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

Unter Windows Vista mit 64 Bit:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

Informationen über die iTunes-Registrierungswerte finden Sie im folgenden Apple-Support-Artikel: http://support.apple.com/kb/HT2102.

Allgemeine Informationen über das Bearbeiten der Windows-Registrierung finden Sie in der Microsoft-Hilfe und im folgenden Support-Artikel: http://support.microsoft.com/kb/136393.

Manuelles Aktualisieren der iTunes- und iPhone OS-Software

Wenn Sie die automatisierte und vom Benutzer zu startende Prüfung auf Softwareaktualisierungen in iTunes deaktivieren, müssen Sie Ihren Benutzern Softwareaktualisierungen zur manuellen Installation bereitstellen.

Informationen zur Aktualisierung von iTunes finden Sie in den weiter vorne in diesem Dokument beschriebenen Schritten zu Installation und Implementierung. Die Vorgehensweise entspricht der Bereitstellung von iTunes für Ihre Benutzer.

Führen Sie die folgenden Schritte aus, um die iPhone OS-Software zu aktualisieren:

1. Laden Sie auf einem Computer, auf dem die Funktion für die iTunes-Softwareaktualisierung nicht deaktiviert ist, die Softwareaktualisierung in iTunes. Wählen Sie dazu in iTunes ein angeschlossenes Gerät aus. Klicken Sie anschließend auf den Titel „Übersicht“ und klicken Sie dann auf die Taste „Nach Update suchen“.
2. Kopieren Sie nach dem Laden die Aktualisierungsdatei (.ipsw), die sich an folgendem Speicherort befindet:
   - *Unter Mac OS X:* ~/Library/iTunes/iPhone Software Updates/
   - *Unter Windows XP: Startlaufwerk*:\Dokumente und Einstellungen*Benutzer*\Anwendungsdaten\Apple Computer\iTunes\iPhone Software Updates\
3. Geben Sie die .ipsw-Datei an Ihre Benutzer weiter oder legen Sie sie im Netzwerk ab, sodass die Benutzer auf die Datei zugreifen können.
4. Fordern Sie die Benutzer auf, vor der Aktualisierung eine Sicherungskopie ihres Geräts mithilfe von iTunes zu erstellen. Bei einer manuellen Aktualisierung legt iTunes vor der Installation nicht automatisch eine Sicherungskopie des Geräts an. Sie erstellen eine neue Sicherungskopie, indem Sie mit der rechten Maustaste (Windows) oder bei gedrückter Taste „ctrl“ (Mac) in der iTunes-Seitenleiste auf das Gerät klicken. Wählen Sie dann „Sichern“ aus dem angezeigten Kontextmenü aus.
5. Ihre Benutzer installieren die Aktualisierung, indem sie ihr Gerät verbinden und dann in iTunes den Titel „Übersicht“ für das Gerät auswählen. Anschließend halten sie die Wahltaste (Mac) oder Umschalttaste (Windows) gedrückt und klicken auf die Taste „Nach Update suchen“.
6. Daraufhin wird ein Dialogfenster für die Dateiauswahl angezeigt. Die Benutzer sollten die .ipsw-Datei auswählen und die Aktualisierung anschließend durch Klicken auf „Öffnen“ starten.

Sichern eines Geräts mit iTunes

Wird ein iPhone, iPod touch oder iPad mit iTunes synchronisiert, werden die Geräteeinstellungen automatisch auf dem Computer gesichert. Programme, die im App Store erworben wurden, werden in die iTunes-Mediathek kopiert.

Programme, die Sie selbst entwickelt und mithilfe von unternehmensspezifischen Profilen an Ihre Benutzer verteilt haben, werden nicht gesichert oder auf den Computer des Benutzers übertragen. Bei der Gerätesicherung werden jedoch alle Datendateien gesichert, die mit Ihren Programmen erstellt wurden.

Die Sicherungskopien von Geräten können in verschlüsselter Form gespeichert werden. Sie müssen dazu nur im Bereich „Übersicht" von iTunes die Option „Backups verschlüsseln" aktivieren. Dateien werden mithilfe von AES256 verschlüsselt. Der Schlüssel wird sicher im iPhone OS-Schlüsselbund gespeichert.

Wichtig: Wenn auf dem Gerät, für das die Sicherungskopie erstellt wird, verschlüsselte Profile installiert sind, wird der Benutzer vom Programm „iTunes" automatisch aufgefordert, die Option zum Verschlüsseln der Sicherungsdaten zu aktivieren.

Bereitstellen von Programmen 5

Sie können iPhone-, iPod touch- und iPad-Programme an Ihre Benutzer verteilen.

Wenn Sie selbst entwickelte iPhone OS-Programme installieren möchten, stellen Sie die Programme für Ihre Benutzer bereit, die sie anschließend mithilfe von iTunes installieren.

Programme aus dem App Store können ohne weitere Konfiguration auf iPhone, iPod touch und iPad genutzt werden. Wenn Sie ein Programm entwickeln, das Sie selbst verteilen möchten, muss es mit einem von Apple ausgestellten Zertifikat digital signiert sein. Außerdem müssen Sie Ihren Benutzern ein Vorlageprofil für die Verteilung bereitstellen, mit dessen Hilfe ihr Gerät das Programm verwenden kann.

Der Prozess für die Bereitstellung und Implementierung eigener Programme umfasst Folgendes:

- Lassen Sie sich bei Apple als Entwickler von Unternehmensprogrammen registrieren.
- Signieren Sie Ihre Programme mithilfe Ihres Zertifikats.
- Erstellen Sie ein Vorlageprofil für die Verteilung im Unternehmen, durch das Geräte zur Verwendung der von Ihnen signierten Programme berechtigt werden.
- Implementieren Sie das Programm und das Vorlageprofil für die Verteilung im Unternehmen auf den Computern Ihrer Benutzer.
- Weisen Sie die Benutzer an, das Programm und das Profil mit iTunes zu installieren.

Details zu den einzelnen Schritten finden Sie in den folgenden Abschnitten.

Registrieren für die Entwicklung von Programmen

Damit Sie eigene Programme für das iPhone OS entwickeln und bereitstellen können, müssen Sie sich unter folgender Adresse für das iPhone Enterprise Developer-Programm registrieren: http://developer.apple.com/.

Nach der Registrierung erhalten Sie Anweisungen, wie Sie Ihre Programme für die Verwendung mit dem iPhone und iPod touch aktivieren.

Signieren von Programmen

Die Programme, die Sie an Benutzer verteilen, müssen mit Ihrem Verteilungszertifikat signiert sein. Anleitungen zum Erhalt und zur Verwendung eines Zertifikats finden Sie im iPhone Developer Center unter der Adresse: http://developer.apple.com/iphone.

Erstellen der Vorlageprofile für die Verteilung

Mithilfe von Vorlageprofilen für die Verteilung können Sie Programme erstellen, die Benutzer auf ihrem Gerät verwenden können. Sie erstellen ein Vorlageprofil für die Verteilung in Ihrem Unternehmen für ein bestimmtes Programm oder für mehrere Programme, indem Sie die AppID angeben, die durch das Profil autorisiert wird. Besitzt ein Benutzer ein Programm, jedoch nicht das zugehörige Profil, das ihn zur Verwendung des Programms berechtigt, kann der Benutzer das Programm nicht nutzen.

Der Ihrem Unternehmen zugewiesene Team Agent kann Vorlageprofile im Enterprise Program Portal unter folgender Adresse erstellen: http://developer.apple.com/iphone. Anleitungen hierzu finden Sie auf der Website.

Nachdem Sie das Vorlageprofil für die Verteilung in Unternehmen erstellt haben, laden Sie die Datei „.mobileprovision“ und sorgen Sie dafür, dass diese Datei zusammen mit Ihren Programmen sicher verteilt wird.

Installieren von Vorlageprofilen mit iTunes

Die installierte iTunes-Kopie des Benutzers installiert Vorlageprofile automatisch, die sich in den im Folgenden beschriebenen Ordnern befinden. Wenn diese Ordner nicht existieren, müssen sie mit den jeweils angegebenen Namen manuell erstellt werden.

Mac OS X

- ~/Library/MobileDevice/Provisioning Profiles/
- /Library/MobileDevice/Provisioning Profiles/
- Pfad, der vom Schlüssel „ProvisioningProfilesPath“ im Ordner „~/Library/Preferences/com.apple.itunes“ angegeben wird

Windows XP

- *Startlaufwerk*:\Dokumente und Einstellungen*Benutzer*\Anwendungsdaten\Apple Computer\MobileDevice\Provisioning Profiles
- *Startlaufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Apple Computer/MobileDevice\Provisioning Profiles
- Pfad, der vom Registrierungsschlüssel „ProvisioningProfilesPath“ mit der Bezeichnung „SOFTWARE\Apple Computer, Inc\iTunes“ im HKCU oder HKLM angegeben wird

Windows Vista

- *Startlaufwerk*:\Benutzer*Benutzername*\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *Startlaufwerk*:\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- Pfad, der vom Registrierungsschlüssel „ProvisioningProfilesPath“ mit der Bezeichnung „SOFTWARE\Apple Computer, Inc\iTunes“ im HKCU oder HKLM angegeben wird

iTunes installiert die an den oben genannten Speicherorten vorhandenen Vorlageprofile automatisch auf den Geräten, die synchronisiert werden. Nach der Installation können die Vorlageprofile auf dem Gerät unter „Einstellungen“ > „Allgemein“ > „Profile“ angezeigt werden.

Sie können auch die Datei „.mobileprovision“ an Ihre Benutzer verteilen und auffordern, die Datei auf das iTunes-Programmsymbol zu bewegen. iTunes kopiert die Datei an den oben angegebenen, korrekten Speicherort.

Installieren von Vorlageprofilen mit dem iPhone-Konfigurationsprogramm

Mit dem iPhone-Konfigurationsprogramm können Sie Vorlageprofile auf angeschlossenen Geräten installieren. Befolgen Sie dazu diese Schritte:

1. Wählen Sie im iPhone-Konfigurationsprogramm „Ablage“ > „Zu Bibliothek hinzufügen“ und wählen Sie das Vorlageprofil aus, das Sie installieren möchten.

   Das Profil wird zum iPhone-Konfigurationsprogramm hinzugefügt und kann durch Auswahl der Kategorie „Vorlageprofile“ in der Bibliothek angezeigt werden.
2. Wählen Sie ein Gerät in der Liste „Verbundene Geräte“ aus.
3. Öffnen Sie durch Klicken den Bereich „Vorlageprofile“.
4. Wählen Sie das Vorlageprofil in der Liste aus und klicken Sie dann auf die zugehörige Taste „Installieren“.

Installieren von Programmen mit iTunes

Ihre Benutzer verwenden iTunes, um Programme auf ihren Geräten zu installieren. Sorgen Sie für eine sichere Verteilung des Programms an Ihre Benutzer und weisen Sie diese an, die folgenden Schritte auszuführen:

1. Wählen Sie in iTunes „Ablage“ > „Zur Mediathek hinzufügen“ und wählen Sie Ihr bereitgestelltes Programm (.app) aus.

   Sie können die .app-Datei auch auf das iTunes-Programmsymbol bewegen.
2. Verbinden Sie ein Gerät mit dem Computer und wählen Sie es in der Liste „Geräte“ in iTunes aus.

3 Klicken Sie auf den Titel „Programme“ und wählen Sie dann das Programm in der Liste aus.

4 Klicken Sie auf „Anwenden“, um das Programm und alle Vorlageprofile für die Verteilung zu installieren, die sich in den im Abschnitt „Installieren von Vorlageprofilen mit iTunes“ auf Seite 74 genannten Ordnern befinden.

Installieren von Programmen mithilfe des iPhone-Konfigurationsprogramms

Mit dem iPhone-Konfigurationsprogramm können Sie Programme auf angeschlossenen Geräten installieren. Befolgen Sie dazu diese Schritte:

1 Wählen Sie im iPhone-Konfigurationsprogramm „Ablage“ > „Zu Bibliothek hinzufügen“ und wählen Sie das Programm aus, das Sie installieren möchten.

Das Programm wird zum iPhone-Konfigurationsprogramm hinzugefügt und kann durch Auswahl der Kategorie „Programme“ in der Bibliothek angezeigt werden.

2 Wählen Sie ein Gerät in der Liste „Verbundene Geräte“ aus.

3 Klicken Sie auf den Titel „Programme“.

4 Wählen Sie das Programm in der Liste aus und klicken Sie dann auf die zugehörige Taste „Installieren“.

Verwenden von unternehmenseigenen Programmen

Wenn ein Benutzer ein Programm verwenden möchte, das nicht von Apple signiert ist, sucht das Gerät nach einem Vorlageprofil, das dessen Verwendung genehmigt. Wird kein Profil gefunden, lässt sich das Programm nicht öffnen.

Deaktivieren eines unternehmenseigenen Programms

Zum Deaktivieren eines unternehmenseigenen Programms müssen Sie die Identität annullieren, mit der das Vorlageprofil für die Verteilung signiert wurde. Das betreffende Programm kann daraufhin nicht mehr installiert werden bzw., sofern es bereits installiert ist, nicht mehr geöffnet werden.

Weitere Informationsquellen

Weitere Informationen zum Erstellen von Programmen und Vorlageprofilen finden Sie hier:

- iPhone Developer Center unter der Adresse: http://developer.apple.com/iphone/

Konfiguration des Cisco-VPN-Servers

Befolgen Sie die hier genannten Richtlinien, um Ihren Cisco-VPN-Server für die Verwendung mit iPhone, iPod touch und iPad zu konfigurieren.

Unterstützte Cisco-Plattformen

Das iPhone OS unterstützt Cisco ASA 5500 Security Appliances und PIX-Firewalls, die mit 7.2.x-Software (oder neuer) konfiguriert sind, wobei das neueste Softwarerelease 8.0.x (oder neuer) empfohlen wird. Das iPhone OS unterstützt außerdem auch Cisco IOS VPN-Router mit IOS Version 12.4(15)T (oder neuer). VPN 3000 Series-Konzentratoren unterstützen die vom iPhone bereitgestellten VPN-Eigenschaften nicht.

Identifizierungsmethoden

Das iPhone OS unterstützt die folgenden Identifizierungsmethoden:

- IPsec-Identifizierung mit Pre-Shared-Schlüssel und einer Benutzeridentifizierung via xauth.
- Client- und Serverzertifikate für IPsec-Identifizierung mit optionaler Benutzeridentifizierung via xauth.
- Hybrid-Identifizierung, bei der vom Server ein Zertifikat und vom Client ein Pre-Shared-Schlüssel für die IPsec-Identifizierung bereitgestellt wird. Die Benutzeridentifizierung erfolgt via xauth.
- Benutzeridentifizierung erfolgt via xauth und umfasst die folgenden Identifizierungsmethoden:
  - Benutzername mit Kennwort
  - RSA-SecurID
  - CryptoCard

Identifizierungsgruppen

Das Cisco Unity-Protokoll verwendet Identifizierungsgruppen, um Benutzer basierend auf einer gängigen Reihe an Identifizierungsparametern und anderen Werten zu gruppieren. Sie sollten eine Identifizierungsgruppe für die Benutzer der iPhone OS-Geräte erstellen. Bei einer Identifizierung mit Pre-Shared-Schlüssel und einer Hybrid-Identifizierung muss der Gruppenname auf dem Gerät so konfiguriert werden, dass der Pre-Shared-Schlüssel („Shared Secret“) der Gruppe als Gruppenkennwort verwendet wird.

Bei der Verwendung der Zertifikatidentifizierung wird kein Schlüssel („Shared Secret“) verwendet und die Gruppe des Benutzers ergibt sich aus den Werten in den Feldern des Zertifikats. Mithilfe der Cisco-Servereinstellungen lassen sich Felder eines Zertifikats Benutzergruppen zuweisen.

Zertifikate

Stellen Sie beim Einrichten und Installieren von Zertifikaten Folgendes sicher:

- Das Identitätszertifikat des Servers muss den DNS-Namen und/oder die IP-Adresse des Servers im Feld für den alternativen Benutzernamen (SubjectAltName) enthalten. Das Gerät überprüft anhand dieser Informationen, ob das Zertifikat zum Server gehört. Sie können den alternativen Benutzernamen mit Platzhalterzeichen angeben, etwa „vpn.*.mycompany.com“, die ein segmentweises Abgleichen und damit mehr Flexibilität ermöglichen. Der DNS-Name kann in das Feld für den allgemeinen Namen eingegeben werden, wenn kein alternativer Benutzername angegeben ist.
- Das Zertifikat der Zertifizierungsinstanz, die das Zertifikat des Servers signierte, muss auf dem Gerät installiert sein. Handelt es sich nicht um ein Root-Zertifikat, installieren Sie den übrigen Teil der Zertifikatskette (Chain of Trust), damit das Zertifikat als vertrauenswürdig gilt.
- Wenn Client-Zertifikate verwendet werden, vergewissern Sie sich, dass das vertrauenswürdige Zertifikat der Zertifizierungsinstanz, die das Zertifikat des Clients signierte, auf dem VPN-Server installiert ist.
- Die Zertifikate und Zertifizierungsinstanzen müssen gültig sein (sie dürfen z. B. nicht abgelaufen sein).
- Das Senden von Zertifikatsketten durch den Server wird nicht unterstützt und sollte deaktiviert werden.
- Vergewissern Sie sich bei der auf Zertifikaten basierenden Identifizierung, dass der Server so konfiguriert ist, dass er die Gruppe des Benutzers basierend auf den jeweiligen Feldern im Client-Zertifikat identifiziert. Beachten Sie hierzu die Informationen im Abschnitt „Identifizierungsgruppen“ auf Seite 78.

IPSec-Einstellungen

Verwenden Sie die folgenden IPSec-Einstellungen:

- *Mode:* Tunnel-Modus
- *IKE Exchange Modes:* „Aggressive Mode“ für die Identifizierung mit Pre-Shared-Schlüssel und für die Hybrid-Identifizierung, „Main Mode“ für die Zertifikatsidentifizierung.
- *Encryption Algorithms:* 3DES, AES-128, AES-256
- *Authentication Algorithms:* HMAC-MD5, HMAC-SHA1
- *Diffie Hellman Groups:* „Group 2“ ist für die Identifizierung mit Pre-Shared-Schlüssel und für die Hybrid-Identifizierung erforderlich. Für die Zertifikatsidentifizierung verwenden Sie „Group 2“ mit 3DES und AES-128. Verwenden Sie „Group 2“ oder „Group 5“ mit AES-256.
- *PFS (Perfect Forward Secrecy):* Für Phase 2 des IKE-Protokolls gilt: Wird PFS verwendet, muss die Diffie-Hellman-Gruppe mit der in Phase 1 des IKE-Protokolls verwendeten Gruppe identisch sein.
- *Mode Configuration:* Muss aktiviert sein.
- *Dead Peer Detection:* Empfohlen.
- *Standard NAT Transversal:* Unterstützt und kann bei Bedarf aktiviert werden. (IPSec over TCP wird nicht unterstützt.)
- *Load Balancing:* Unterstützt und kann bei Bedarf aktiviert werden.
- *Re-keying of Phase 1:* Derzeit nicht unterstützt. Es wird empfohlen, das Rekeying-Intervall für die erneute Aushandlung der Schlüssel auf ungefähr eine Stunde einzustellen.
- *ASA Address Mask:* Stellen Sie sicher, dass alle Masken des Geräte-Adress-Pools entweder nicht festgelegt oder auf 255.255.255.255 eingestellt sind. Beispiel:

  ```
  asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask
     255.255.255.255.
  ```

  Wenn Sie die empfohlene Adressmaske verwenden, werden unter Umständen einige der von der VPN-Konfiguration angenommenen Routen ignoriert. Dies kann vermieden werden, indem Sie sicherstellen, dass die Routing-Tabelle alle erforderlichen Routen enthält, und indem Sie vor der Implementierung prüfen, ob die Teilnetzadressen zugänglich sind.

Andere unterstützte Funktionen

iPhone, iPod touch und iPad unterstützen Folgendes:

- *Application Version:* Die Software-Version des Clients wird an den Server gesendet, sodass der Server Verbindungen basierend auf der Softwareversion des Geräts akzeptieren oder ablehnen kann.
- *Banner:* Das Banner wird, sofern es auf dem Server konfiguriert ist, auf dem Gerät angezeigt und der Benutzer muss es akzeptieren oder die Verbindung trennen.
- *Split Tunnel:* Split-Tunneling wird unterstützt.
- *Split DNS:* Split-DNS wird unterstützt.
- *Default Domain:* Die Standard-Domain wird unterstützt.

Format von Konfigurationsprofilen

Dieser Anhang enthält Informationen zum Format von mobileconfig-Dateien für Benutzer, die eigene Programme entwickeln möchten.

In diesem Kapitel wird vorausgesetzt, dass Sie mit der Apple XML DTD (Document Type Definition) und dem allgemeinen .plist-Format (Property List, Eigenschaftsliste) vertraut sind. Eine allgemeine Beschreibung des .plist-Formats von Apple finden Sie unter: www.apple.com/DTDs/PropertyList-1.0.dtd. Erstellen Sie zu Beginn mit dem iPhone-Konfigurationsprogramm eine Gerüstdatei, die Sie anhand der Informationen in diesem Anhang bearbeiten können.

Im vorliegenden Anhang werden die Begriffe *Payload-Segment* und *Profil* verwendet. Ein Profil bezeichnet die gesamte Datei, mit der bestimmte (einzelne oder mehrere) Einstellungen auf iPhone, iPod touch oder iPad konfiguriert werden. Unter Payload-Segment versteht man eine einzelne Komponente der Profildatei.

Root-Ebene

Auf Root-Ebene ist die Konfigurationsdatei ein Funktionsverzeichnis mit den folgenden Schlüssel-/Wertpaaren:

Schlüssel	Wert
PayloadVersion	Nummer, obligatorisch. Dies ist die Version des gesamten Konfigurationsprofils. Diese Versionsnummer bestimmt das Format des gesamten Profils, nicht der einzelnen Payload-Segmente.
PayloadUUID	Zeichenkette, obligatorisch. Hierbei handelt es sich meist um eine synthetisch generierte, eindeutige ID-Zeichenkette. Der genaue Inhalt dieser Zeichenkette spielt keine Rolle. Wichtig ist jedoch, dass sie immer eindeutig ist. Unter Mac OS X können Sie UUIDs mit /usr/bin/uuidgen generieren.
PayloadType	Zeichenkette, obligatorisch. Derzeit ist nur „Configuration“ ein gültiger Wert für diesen Schlüssel.
PayloadOrganization	Zeichenkette, optional. Dieser Wert beschreibt die das Profil ausstellende Organisation, wie diese dem Benutzer angezeigt wird.

Schlüssel	Wert
PayloadIdentifier	Zeichenkette, obligatorisch. Dieser Wert ist standardmäßig eine durch Punkte getrennte Zeichenkette, die das Profil eindeutig beschreibt, etwa „com.myCorp.iPhone.mailSettings“ oder „edu.myCollege.students.vpn“. Anhand dieser Zeichenkette werden Profile unterschieden. Wird ein Profil installiert, dessen ID der eines anderen Profils entspricht, wird dieses Profil überschreiben (und nicht hinzugefügt).
PayloadDisplayName	Zeichenkette, obligatorisch. Mit diesem Wert wird eine sehr kurze Zeichenkette bestimmt, die dem Benutzer als Beschreibung des Profils angezeigt wird, z. B. „VPN-Einstellungen“. Sie muss nicht eindeutig sein.
PayloadDescription	Zeichenkette, optional. Mit diesem Wert wird bestimmt, welcher beschreibende Freiformtext dem Benutzer im Bildschirm „Details“ für das gesamte Profil angezeigt wird. Die Zeichenkette sollte das Profil klar identifizieren, damit der Benutzer entscheiden kann, ob er es installieren möchte.
PayloadContent	Datenfeld, optional. Dieser Wert entspricht dem tatsächlichen Inhalt des Profils. Wird er ausgelassen, ist das gesamte Profil ohne Funktion.
PayloadRemovalDisallowed	Boolesch, optional. Der Standardwert ist „No“. Das Aktivieren bedeutet, dass der Benutzer das Profil nicht löschen kann. Ein Profil, für das diese Festlegung gilt, kann per USB oder Web/E-Mail nur aktualisiert werden, wenn die Kennung des vorhandenen Profils mit der Kennung des aktualisierten Profils übereinstimmt und die Signierung durch dieselbe Zertifizierungsstelle erfolgt. Wird ein Kennwort festgelegt, kann das Profil gelöscht werden, wenn das Kennwort als Berechtigungsnachweis eingegeben wird. Im Falle eines signierten und verschlüsselten Profils ist die Anzeige dieses Sperrbits ohne Folgen, da das Profil nicht geändert werden kann, weshalb die Einstellung auch auf dem Gerät zu sehen ist.

Payload-Segment „Content“

Das Datenfeld „PayloadContent“ besteht aus Funktionsverzeichnissen, die alle ein individuelles Payload-Segment des Profils beschreiben. Zu jedem funktionierenden Profil ist in diesem Datenfeld mindestens ein Eintrag vorhanden. Alle Funktionsverzeichnisse im Datenfeld haben einige gemeinsame Eigenschaften, unabhängig vom Payload-Typ. Andere sind speziell auf die einzelnen Payload-Typen abgestimmt und eindeutig.

Schlüssel	Wert
PayloadVersion	Nummer, obligatorisch. Dies ist die Version des jeweiligen Payload-Segments. Alle Profile können aus Payload-Segmenten mit verschiedenen Versionsnummern bestehen. Die VPN-Versionsnummer könnte beispielsweise ab einem bestimmten Zeitpunkt schrittweise erhöht werden, die Mail-Versionsnummer dagegen nicht.
PayloadUUID	Zeichenkette, obligatorisch. Hierbei handelt es sich meist um eine synthetisch generierte, eindeutige ID-Zeichenkette. Der genaue Inhalt dieser Zeichenkette spielt keine Rolle. Wichtig ist jedoch, dass sie immer eindeutig ist.
PayloadType	Zeichenkette, obligatorisch. Mit diesem Schlüssel-/Wertepaar wird der Typ des einzelnen Payload-Segments im Profil bestimmt.
PayloadOrganization	Zeichenkette, optional. Dieser Wert beschreibt die das Profil ausstellende Organisation, wie diese dem Benutzer angezeigt wird. Der Wert kann, muss aber nicht, mit dem Wert „PayloadOrganization“ der Root-Ebene identisch sein.
PayloadIdentifier	Zeichenkette, obligatorisch. Dieser Wert ist standardmäßig eine durch Punkte getrennte Zeichenkette, die das Payload-Segment eindeutig beschreibt. Meist handelt es sich um den Wert „PayloadIdentifier“ auf Root-Ebene mit einer angehängten Sub-ID, die das jeweilige Payload-Segment beschreibt.
PayloadDisplayName	Zeichenkette, obligatorisch. Dieser Wert ist eine sehr kurze Zeichenkette, die dem Benutzer angezeigt wird und die das Profil beschreibt, etwa „VPN-Einstellungen“. Sie muss nicht eindeutig sein.
PayloadDescription	Zeichenkette, optional. Mit diesem Wert wird bestimmt, welcher beschreibende Freiformtext im Bildschirm „Details“ für dieses bestimmte Payload-Segment angezeigt wird.

Payload-Segment „Removal Password“

Das Payload-Segment „Removal Password“ wird vom PayloadType-Wert „com.apple.profileRemovalPassword“ bestimmt. Es wird zum Verschlüsseln des Kennworts verwendet, das einem Benutzer als Berechtigungsnachweis dafür dient, ein Konfigurationsprofil vom Gerät zu entfernen. Wenn dieses Payload-Segment vorhanden und ein Kennwort festgelegt wird, wird der Benutzer vom iPhone aufgefordert, das betreffende Kennwort einzugeben, wenn er auf „Entfernen“ tippt. Dieses Payload-Segment wird zusammen mit den übrigen Informationen des Profils verschlüsselt.

Schlüssel	Wert
RemovalPassword	Zeichenkette, optional. Diese Wert ist das Kennwort, das als Berechtigungsnachweis zum Löschen des Profils eingegeben werden muss.

Payload-Segment „Passcode Policy“

Das Payload-Segment „Passcode Policy“ wird durch den PayloadType-Wert „com.apple.mobiledevice.passwordpolicy“ bestimmt. Ist dieser Payload-Typ vorhanden, wird das Gerät aufgefordert, dem Benutzer einen Mechanismus zur Eingabe eines alphanumerischen Codes anzubieten, der die Eingabe von Codes mit beliebiger Länge und Komplexität erlaubt.

Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
allowSimple	Boolesch, optional. Der Standardwert ist „YES“. Dieser Wert bestimmt, ob ein einfacher Code zulässig ist. Ein einfacher Code enthält sich wiederholende Zeichen oder auf- bzw. absteigende Zeichen (wie 123 oder CBA). Der Wert „NO“ ist gleichbedeutend mit der Einstellung von „minComplexChars“ auf „1“.
forcePIN	Boolesch, optional. Der Standardwert ist „NO“. Dieser Wert bestimmt, ob der Benutzer eine PIN-Nummer festlegen muss. Das Festlegen dieses Werts (und keiner anderen Werte) bewirkt, dass der Benutzer einen Code eingeben muss. Länge oder Sicherheit des Codes sind dabei nicht vorgegeben.
maxFailedAttempts	Nummer, optional. Der Standardwert ist „11“, der zulässige Bereich ist [2...11]. Dieser Wert gibt die Anzahl zulässiger Fehlversuche bei der Eingabe des Codes zur Freigabe des gesperrten Geräts an. Nachdem diese Anzahl überschritten ist, wird das Gerät gesperrt und muss mit dem Computer mit der passenden iTunes-Kopie verbunden werden, damit die Sperre aufgehoben werden kann.

Schlüssel	Wert
maxInactivity	Nummer, optional. Der Standardwert ist „Infinity“. Dieser Wert gibt an, wie viele Minuten das Gerät unbenutzt sein kann (ohne vom Benutzer gesperrt zu werden), bevor es vom System gesperrt wird. Wird diese Grenze erreicht, wird das Gerät gesperrt und die Eingabe des Codes ist erforderlich.
maxPINAgeInDays	Nummer, optional. Der Standardwert ist „Infinity“. Gibt an, wie viele Tage der Code ohne Änderung beibehalten werden kann. Nach Ablauf der festgelegten Anzahl von Tagen muss der Benutzer den Code ändern, um das Gerät freigeben zu können.
minComplexChars	Nummer, optional. Der Standardwert ist „0“. Dieser Wert gibt an, wie viele komplexe Zeichen der Code mindestens enthalten muss. Ein komplexes Zeichen ist ein Zeichen, das weder Buchstabe noch Zahl ist, z. B. &%$#.
minLength	Nummer, optional. Der Standardwert ist „0“. Dieser Wert gibt die minimale allgemeine Länge des Codes an. Dieser Parameter ist unabhängig vom ebenfalls optionalen Argument „minComplexChars“.
requireAlphanumeric	Boolesch, optional. Der Standardwert ist „NO“. Dieser Wert gibt an, ob der Benutzer alphabetische Zeichen („abcd“) eingeben muss oder ob Zahlen ausreichend sind.
pinHistory	Nummer, optional. Dieser Wert gibt an, wie viele frühere Codes für den Vergleich herangezogen werden sollen, mit dem bestimmt wird, ob ein vom Benutzer festgelegter neuer Code eindeutig ist. Der Mindestwert ist „1“, der Maximalwert ist „50“.
manualFetchingWhenRoaming	Boolesch, optional. Das Aktivieren bedeutet, dass beim Roaming alle Push-Operationen unterbunden werden. Der Benutzer muss neue Daten manuell abrufen.
maxGracePeriod	Nummer, optional. Dies ist die maximale Zeitspanne (in Minuten), während der die Sperre des Telefons aufgehoben werden kann, ohne dass dafür der Code eingegeben werden muss. Der Standardwert ist „0“; er bedeutet, dass es keine Kulanzzeit gibt und der Code sofort eingegeben werden muss.

Payload-Segment „Email“

Das Payload-Segment „Email“ wird vom PayloadType-Wert „com.apple.mail.managed“ bestimmt. Mit diesem Payload-Segment wird ein E-Mail-Account auf dem Gerät erstellt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
EmailAccountDescription	Zeichenkette, optional. Dies ist eine für Benutzer sichtbare Beschreibung des E-Mail-Accounts, die in den Programmen „Mail“ und „Einstellungen“ angezeigt wird.
EmailAccountName	Zeichenkette, optional. Dies ist der vollständige Benutzername des Accounts. Dieser Name wird in gesendeten Nachrichten etc. verwendet.
EmailAccountType	Zeichenkette, obligatorisch. Die zulässigen Werte sind „EmailTypePOP“ und „EmailTypeIMAP“. Dieser Wert definiert das für diesen Account zu verwendende Protokoll.
EmailAddress	Zeichenkette, obligatorisch. Dieser Wert bestimmt die vollständige E-Mail-Adresse für den Account. Fehlt diese Angabe im Payload-Segment, fordert das Gerät die Adresse bei der Installation des Profils an.
IncomingMailServerAuthentication	Zeichenkette, obligatorisch. Dieser Wert bestimmt das Identifizierungsschema für eingehende E-Mails. Die zulässigen Werte sind „EmailAuthPassword“ und „EmailAuthNone“.
IncomingMailServerHostName	Zeichenkette, obligatorisch. Dieser Wert bestimmt den Hostnamen (oder die IP-Adresse) des Servers für eingehende E-Mails.
IncomingMailServerPortNumber	Nummer, optional. Dieser Wert bestimmt die Portnummer des Servers für eingehende E-Mails. Wird keine Portnummer angegeben, wird der Standardport für das jeweilige Protokoll verwendet.
IncomingMailServerUseSSL	Boolesch, optional. Der Standardwert ist „YES“. Dieser Wert bestimmt, ob der Server für eingehende E-Mails SSL für die Identifizierung verwendet.
IncomingMailServerUsername	Zeichenkette, obligatorisch. Dieser Wert bestimmt den Benutzernamen für den E-Mail-Account, der bis zum @-Zeichen meist mit der E-Mail-Adresse identisch ist. Wenn die Zeichenkette nicht im Payload-Segment vorhanden ist und der Account so konfiguriert ist, dass für eingehende E-Mails eine Identifizierung erforderlich ist, fordert das Gerät diese Zeichenkette während der Installation des Profils an.
IncomingPassword	Zeichenkette, optional. Dies ist das Kennwort für den Server für eingehende E-Mails. Geben Sie diesen Wert nur bei verschlüsselten Profilen an.
OutgoingPassword	Zeichenkette, optional. Dies ist das Kennwort für den Server für ausgehende E-Mails. Geben Sie diesen Wert nur bei verschlüsselten Profilen an.

Schlüssel	Wert
OutgoingPasswwordSameAsIncomingPassword	Boolesch, optional. Das Aktivieren bedeutet, dass der Benutzer nur ein einmal zur Eingabe des Kennworts aufgefordert wird, da das Kennwort gleichermaßen für ein- und für ausgehende E-Mails verwendet wird.
OutgoingMailServerAuthentication	Zeichenkette, obligatorisch. Dieser Wert bestimmt das Identifizierungsschema für ausgehende E-Mails. Die zulässigen Werte sind „EmailAuthPassword“ und „EmailAuthNone“.
OutgoingMailServerHostName	Zeichenkette, obligatorisch. Dieser Wert bestimmt den Hostnamen (oder die IP-Adresse) des Servers für ausgehende E-Mails.
OutgoingMailServerPortNumber	Nummer, optional. Dieser Wert bestimmt die Portnummer des Servers für ausgehende E-Mails. Wird keine Portnummer angegeben, werden nacheinander die Ports 25, 587 und 465 verwendet.
OutgoingMailServerUseSSL	Boolesch, optional. Der Standardwert ist „YES“. Dieser Wert bestimmt, ob der Server für ausgehende E-Mails SSL für die Identifizierung verwendet.
OutgoingMailServerUsername	Zeichenkette, obligatorisch. Dieser Wert bestimmt den Benutzernamen für den E-Mail-Account, der bis zum @-Zeichen meist mit der E-Mail-Adresse identisch ist. Wenn die Zeichenkette nicht im Payload-Segment vorhanden ist und der Account so konfiguriert ist, dass für ausgehende E-Mails eine Identifizierung erforderlich ist, fordert das Gerät diese Zeichenkette während der Installation des Profils an.

Payload-Segment „Web Clip“

Das Payload-Segment „Web Clip“ wird vom PayloadType-Wert „com.apple.webClip.managed“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
URL	Zeichenkette, obligatorisch. Dies ist die URL, die beim Klicken auf den Web-Clip geöffnet werden soll. Die URL muss mit dem Präfix „HTTP“ oder „HTTPS“ beginnen, da der Web-Clip sonst nicht funktioniert.
Label	Zeichenkette, obligatorisch. Dies ist der Name, mit dem der Web-Clip im Home-Bildschirm angezeigt wird.
Icon	Daten, optional. Dies ist das Symbol im Format PNG, das im Home-Bildschirm angezeigt wird. Die Größe sollte 59 x 60 Pixel betragen. Wird dieser Wert nicht angegeben, wird ein weißes Rechteck angezeigt.
IsRemovable	Boolesch, optional. Der Wert „No“ bedeutet, dass der Benutzer den Web-Clip nicht entfernen kann; der Web-Clip wird aber entfernt, wenn das Profil gelöscht wird.

Payload-Segment „Restrictions“

Das Payload-Segment „Restrictions“ wird vom PayloadType-Wert „com.apple.applicationaccess“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
allowAppInstallation	Boolesch, optional. Ist dieser Wert falsch, wird der App Store deaktiviert und sein Symbol vom Home-Bildschirm entfernt. Benutzer können ihre Programme nicht installieren oder aktualisieren.
allowCamera	Boolesch, optional. Ist dieser Wert falsch, wird die Kamera vollständig deaktiviert und ihr Symbol vom Home-Bildschirm entfernt. Benutzer können in diesem Fall keine Fotos aufnehmen.
allowExplicitContent	Boolesch, optional. Ist dieser Wert falsch, werden im iTunes Store erworbene anstößige Musik- und Videotitel nicht angezeigt. Für Titel, die im iTunes Store angeboten werden, erfolgt gegebenenfalls die Kennzeichnung als „Anstößig“ durch den jeweiligen Inhalteanbieter (Content Provider).
allowScreenShot	Boolesch, optional. Ist dieser Wert falsch, können Benutzer kein Bildschirmfoto der Anzeige sichern.
allowYouTube	Boolesch, optional. Ist dieser Wert falsch, wird das Programm „YouTube“ deaktiviert und sein Symbol vom Home-Bildschirm entfernt.
allowiTunes	Boolesch, optional. Ist dieser Wert falsch, wird der iTunes Musik Store deaktiviert und sein Symbol vom Home-Bildschirm entfernt. Benutzer sind in diesem Fall nicht in der Lage, Inhalte in der Vorschau anzusehen, anzuhören, zu kaufen oder herunterzuladen.
allowSafari	Boolesch, optional. Ist dieser Wert falsch, wird das Webbrowser-Programm „Safari“ deaktiviert und sein Symbol vom Home-Bildschirm entfernt. Benutzer können in diesem Fall keine Webclips öffnen.

Payload-Segment „LDAP“

Das Payload-Segment „LDAP“ wird vom PayloadType-Wert „com.apple.ldap.account“ bestimmt. Zwischen dem LDAP-Account und dem Parameter „LDAPSearchSettings“ besteht eine 1-zu-viele-Beziehung. Stellen Sie sich LDAP als eine Baumstruktur vor. Jedes „SearchSettings“-Objekt stellt einen Knoten innerhalb dieser Struktur dar, ab dem die Suche erfolgt und der Suchmodus greift (Knoten ODER Knoten + 1 untergeordnete Ebene ODER Knoten + alle untergeordneten Ebenen). Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
LDAPAccountDescription	Zeichenkette, optional. Dies ist die Beschreibung des Accounts.
LDAPAccountHostName	Zeichenkette, obligatorisch. Dies ist der Name des Hosts.
LDAPAccountUseSSL	Boolesch, obligatorisch. Dieser Wert bestimmt, ob SSL verwendet wird oder nicht.

Schlüssel	Wert
LDAPAccountUserName	Zeichenkette, optional. Dies ist der Benutzernamen.
LDAPAccountPassword	Zeichenkette, optional. Geben Sie diesen Wert nur bei verschlüsselten Profilen an.
LDAPSearchSettings	Dies ist das Container-Objekt auf der obersten Ebene. Für einen einzelnen Account können mehrere solche Objekte vorhanden sein. Damit der Account sinnvoll verwendet werden kann, muss mindestens ein Objekt vorhanden sein.
LDAPSearchSettingDescription	Zeichenkette, optional. Dies ist die Beschreibung der Sucheinstellung.
LDAPSearchSettingSearchBase	Zeichenkette, obligatorisch. Dies ist von der Konzeption der Pfad zu dem Knoten unter „ou=people,o=example corp“, ab dem die Suche erfolgen soll.
LDAPSearchSettingScope	Zeichenkette, obligatorisch. Dieser Wert bestimmt das rekursive Element der Suche. Die folgenden drei Werte sind möglich: LDAPSearchSettingScopeBase: Die Suche bleibt auf den Knoten beschränkt, der mit dem Parameter „SearchBase“ definiert wird. LDAPSearchSettingScopeOneLevel: Der Knoten und die ihm direkt untergeordnete Ebene werden durchsucht. LDAPSearchSettingScopeSubtree: Der Knoten und alle ihm untergeordnete Ebenen (unabhängig von der Tiefe der Verschachtelung) werden durchsucht.

Payload-Segment „CalDAV“

Das Payload-Segment „CalDAV“ wird vom PayloadType-Wert „com.apple.caldav.account“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
CalDAVAccountDescription	Zeichenkette, optional. Dies ist die Beschreibung des Accounts.
CalDAVHostName	Zeichenkette, obligatorisch. Dies ist die Adresse des Servers.
CalDAVUsername	Zeichenkette, obligatorisch. Dies ist der Anmeldename des Benutzers.
CalDAVPassword	Zeichenkette, optional. Dies ist das Kennwort des Benutzers.
CalDAVUseSSL	Boolesch, obligatorisch. Dieser Wert bestimmt, ob SSL verwendet wird oder nicht.
CalDAVPort	Nummer, optional. Dies ist der Port, über den die Verbindung zum Server hergestellt werden soll.
CalDAVPrincipalURL	Zeichenkette, optional. Dies ist die Basis-URL für den Kalender des Benutzers.

Payload-Segment „Calendar Subscription“

Das Payload-Segment „CalSub“ wird vom PayloadType-Wert „com.apple.subscribed-calendar.account“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
SubCalAccountDescription	Zeichenkette, optional. Dies ist die Beschreibung des Accounts.
SubCalAccountHostName	Zeichenkette, obligatorisch. Dies ist die Adresse des Servers.
SubCalAccountUsername	Zeichenkette, optional. Dies ist der Anmeldename des Benutzers.
SubCalAccountPassword	Zeichenkette, optional. Dies ist das Kennwort des Benutzers.
SubCalAccountUseSSL	Boolesch, obligatorisch. Dieser Wert bestimmt, ob SSL verwendet wird oder nicht.

Payload-Segment „SCEP“

Das Payload-Segment „SCEP“ (Simple Certificate Enrollment Protocol) wird vom PayloadType-Wert „com.apple.encrypted-profile-service“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
URL	Zeichenkette, obligatorisch.
Name	Zeichenkette, optional. Hierbei kann es sich um eine beliebige Zeichenkette handeln, die vom SCEP-Server verstanden wird. Beispielsweise könnte ein Domänenname (z. B. „example.org“) verwendet werden. Wenn eine Zertifizierungsstelle (CA) mehrere CA-Zertifikate bereitstellt, kann mit diesem Feld angegeben werden, welches dieser Zertifikate benötigt wird.
Betreff	Datenfeld, optional. Hierbei handelt es sich um die Darstellung eines X.500-Namens in Form eines Datenfelds aus OID und Wert. Beispiel: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar – Die übersetzte Form sieht wie folgt aus: [[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]] OIDs können durch Zahlen mit Punkten dargestellt werden; als Kürzel können C, L, ST, O, OU, CN verwendet werden (für Country [Staat], Locality [Ort], State [Bundesstaat/-land], Organization [Behörde/Organisation], Organizational Unit [Organisationseinheit], Common Name [Servername]).
Challenge	Zeichenkette, optional. Hierbei handelt es sich um ein so genanntes Pre-Shared Secret.
Keysize	Nummer, optional. Dies ist die Schlüsselgröße in Bit; mögliche Werte sind „1024“ und „2048“.

Schlüssel	Wert
Key Type	Zeichenkette, optional. Derzeit ist nur „RSA“ gültig.
Key Usage	Nummer, optional. Eine Bitmaske, die die Nutzung des Schlüssels angibt. “1“ steht für Signieren, „4“ steht für Verschlüsseln und „5“ steht für Signieren und Verschlüsseln. Einige Zertifizierungsstellen wie Windows-Zertifizierungsstellen unterstützen nur die Verschlüsselung oder die Signierung, aber nicht beides gleichzeitig.

Schlüssel „SubjectAltName“ für das Funktionsverzeichnis

Das Payload-Segment „SCEP“ kann ein optionales Funktionsverzeichnis „SubjectAltName“ angeben, das Werte bereitstellt, die von der Zertifizierungsstelle für die Ausgabe eines Zertifikats benötigt werden. Sie können eine einzelne Zeichenfolge oder eine Reihe von Zeichenfolgen für jeden Schlüssel definieren. Welche Werte Sie angeben, hängt von der verwendeten Zertifizierungsstelle ab. Möglicherweise enthalten sind DNS-Name, URL oder E-Mail-Werte. Ein Beispiel finden Sie unter „Muster für Phase 3 – Antwort des Servers mit SCEP-Spezifikationen“ auf Seite 99.

Schlüssel „GetCACaps“ für das Funktionsverzeichnis

Wenn Sie ein Funktionsverzeichnis mit dem Schlüssel „GetCACaps“ hinzufügen, verwendet das Gerät die angegebenen Zeichenfolgen als maßgebliche Informationsquelle über die Fähigkeiten Ihrer Zertifizierungsstelle. Andernfalls ragt das Gerät den Schlüssel „GetCACaps“ bei der Zertifizierungsstelle ab und verwendet die dabei erhaltene Antwort. Reagiert die Zertifizierungsstelle nicht, verwendet das Gerät standardmäßig GET 3DES- und SHA-1-Anforderungen.

Payload-Segment „APN“

Das Payload-Segment „APN“ (Access Point Name) wird durch den PayloadType-Wert „com.apple.apn.managed“ bestimmt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
DefaultsData	Funktionsverzeichnis, obligatorisch. Dieses Funktionsverzeichnis enthält zwei Schlüssel-/Wertepaare.
DefaultsDomainName	Zeichenkette, obligatorisch. Der einzig zulässige Wert ist „com.apple.managedCarrier“.
apns	Datenfeld, obligatorisch. Dieses Datenfeld enthält eine zufällig gewählte Anzahl Funktionsverzeichnisse, die alle eine APN-Konfiguration beschreiben, mit den Schlüssel-/Wertepaaren darunter.
apn	Zeichenkette, obligatorisch. Diese Zeichenkette gibt den APN (Access Point Name, Name des Netzbetreibers) an.

Schlüssel	Wert
username	Zeichenkette, obligatorisch. Diese Zeichenkette gibt den Benutzernamen für diesen APN an. Fehlt diese Angabe, fordert das Gerät den Namen bei der Installation des Profils an.
password	Daten, optional. Bei diesen Daten handelt es sich um das Kennwort des Benutzers für diesen APN. Es ist aus Sicherheitsgründen codiert. Fehlt diese Angabe im Payload-Segment, fordert das Gerät das Kennwort bei der Installation des Profils an.
proxy	Zeichenkette, optional. Dies ist die IP-Adresse oder die URL des APN-Proxy-Servers.
proxyPort	Nummer, optional. Dies ist die Nummer des Ports des APN-Proxy-Servers.

Payload-Segment „Exchange“

Das Payload-Segment „Exchange“ wird vom PayloadType-Wert „com.apple.eas.account“ bestimmt. Mit diesem Payload-Segment wird ein Microsoft Exchange-Account auf dem Gerät erstellt. Neben den für alle Payload-Segmente geltenden Einstellungen definiert dieses Payload-Segment Folgendes:

Schlüssel	Wert
EmailAddress	Zeichenkette, obligatorisch. Fehlt diese Angabe im Payload-Segment, fordert das Gerät die Adresse bei der Installation des Profils an. Dieser Wert bestimmt die vollständige E-Mail-Adresse für den Account.
Host	Zeichenkette, obligatorisch. Dieser Wert bestimmt den Hostnamen (oder die IP-Adresse) des Exchange-Servers.
SSL	Boolesch, optional. Der Standardwert ist „YES“. Dieser Wert bestimmt, ob der Exchange-Server SSL für die Identifizierung verwendet.
UserName	Zeichenkette, obligatorisch. Diese Zeichenkette gibt den Benutzernamen für diesen Exchange-Account an. Fehlt diese Angabe, fordert das Gerät die Zeichenkette bei der Installation des Profils an.
Kennwort	Zeichenkette, optional. Dies ist das Kennwort des Accounts. Geben Sie diesen Wert nur bei verschlüsselten Profilen an.
Certificate	Optional. Hierbei handelt es sich um ein .p12-Identitätszertifikat im NSData-blob-Format für Accounts, die die Identifizierung per Zertifikat zulassen.
CertificateName	Zeichenkette, optional. Gibt den Namen oder die Beschreibung des Zertifikats an.
CertificatePassword	Optional. Dies ist das für das .p12-Identitätszertifikat benötigte Kennwort. Geben Sie diesen Wert nur bei verschlüsselten Profilen an.

Payload-Segment „VPN“

Das Payload-Segment „VPN“ wird vom PayloadType-Wert „com.apple.vpn.managed“ bestimmt. Zusätzlich zu den Einstellungen, die für alle Payload-Typen gleichermaßen gelten, definiert das Payload-Segment „VPN“ die folgenden Schlüssel.

Schlüssel	Wert
UserDefinedName	Zeichenkette. Dies ist die Beschreibung der auf dem Gerät angezeigten VPN-Verbindung.
OverridePrimary	Boolesch. Dieser Wert legt fest, ob der gesamte Datenverkehr über die VPN-Schnittstelle übertragen werden soll. Beim Wert „TRUE“ wird der gesamte Netzwerkverkehr über VPN gesendet.
VPNType	Zeichenkette. Dieser Wert bestimmt die Einstellungen, die im Payload-Segment für diesen VPN-Verbindungstyp verfügbar sind. Drei Werte sind möglich: „L2TP“, „PPTP“ oder „IPSec“ jeweils für L2TP, PPTP und Cisco IPSec.

Auf der obersten Ebene sind zwei mögliche Funktionsverzeichnisse vorhanden, und zwar unter den Schlüsseln „PPP“ und „IPSec“. Die Schlüssel in diesen beiden Funktionsverzeichnissen werden im Folgenden zusammen mit dem VPNType-Wert beschrieben, unter dem die Schlüssel verwendet werden.

PPP-Schlüssel für das Funktionsverzeichnis

Die folgenden Elemente gelten für VPN-Payload-Segmente des Typs „PPP“.

Schlüssel	Wert
AuthName	Zeichenkette. Dies ist der Benutzername des VPN-Accounts. Dieser Wert wird für L2TP und PPTP verwendet.
AuthPassword	Zeichenkette, optional. Dieser Wert ist nur sichtbar, wenn für „TokenCard“ der Wert „FALSE“ eingestellt ist. Dieser Wert wird für L2TP und PPTP verwendet.
TokenCard	Boolesch. Dieser Wert gibt an, ob eine Token-Karte wie eine RSA-SecurID-Karte für den Verbindungsaufbau verwendet wird. Dieser Wert wird für L2TP verwendet.
CommRemoteAddress	Zeichenkette. Dies ist die IP-Adresse oder der Hostname des VPN-Servers. Dieser Wert wird für L2TP und PPTP verwendet.
AuthEAPPlugins	Datenfeld. Dieses Feld ist nur vorhanden, wenn RSA-SecurID verwendet wird. In diesem Fall ist ein (1) Eintrag vorhanden; es handelt sich dabei um eine Zeichenkette mit dem Wert „EAP-RSA“. Dieser Wert wird für L2TP und PPTP verwendet.
AuthProtocol	Datenfeld. Dieses Feld ist nur vorhanden, wenn RSA-SecurID verwendet wird. In diesem Fall ist ein (1) Eintrag vorhanden; es handelt sich dabei um eine Zeichenkette mit dem Wert „EAP-RSA“. Dieser Wert wird für L2TP und PPTP verwendet.
CCPMPPE40Enabled	Boolesch. Vgl. Angaben zum Schlüssel „CCPEnabled“. Dieser Wert wird für PPTP verwendet.

Schlüssel	Wert
CCPMPPE128Enabled	Boolesch. Vgl. Angaben zum Schlüssel „CCPEnabled“. Dieser Wert wird für PPTP verwendet.
CCPEnabled	Boolesch. Dieser Schlüssel aktiviert die Verschlüsselung der Verbindung. Haben dieser Schlüssel und der Schlüssel „CCPMPPE40Enabled“ den Wert „TRUE“, repräsentiert er die automatische Verschlüsselungsebene. Haben dieser Schlüssel und der Schlüssel „CCPMPPE128Enabled“ den Wert „TRUE“, repräsentiert er die maximale Verschlüsselungsebene. Wird keine Verschlüsselung verwendet, hat keiner der CCP-Schlüssel den Wert „TRUE“. Dieser Wert wird für PPTP verwendet.

IPSec-Schlüssel für das Funktionsverzeichnis

Die folgenden Elemente gelten für VPN-Payload-Segmente des Typs „IPSec“.

Schlüssel	Wert
RemoteAddress	Zeichenkette. Dies ist die IP-Adresse oder der Hostname des VPN-Servers. Dieser Wert wird für Cisco IPSec verwendet.
AuthenticationMethod	Zeichenkette. Dieser Wert lautet entweder „SharedSecret“ oder „Certificate“. Dieser Wert wird für L2TP und Cisco IPSec verwendet.
XAuthName	Zeichenkette. Dies ist der Benutzername des VPN-Accounts. Dieser Wert wird für Cisco IPSec verwendet.
XAuthEnabled	Ganzzahl. Der Wert ist „1“, wenn „XAUTH=ON“ (aktiviert) ist, er ist „0“, wenn „XAUTH=OFF“ (deaktiviert) ist. Dieser Wert wird für Cisco IPSec verwendet.
LocalIdentifier	Zeichenkette. Dieser Wert ist nur vorhanden, wenn „AuthenticationMethod=SharedSecret“ ist. Dies ist der Name der zu verwendenden Gruppe. Bei Verwendung der Hybrid-Identifizierung muss die Zeichenkette mit „[hybrid]“ enden. Dieser Wert wird für Cisco IPSec verwendet.
LocalIdentifierType	Zeichenkette. Dieser Wert ist nur vorhanden, wenn „AuthenticationMethod=SharedSecret“ ist. Der Wert lautet „KeyID“. Dieser Wert wird für L2TP und Cisco IPSec verwendet.
SharedSecret	Daten. Dies ist der Schlüssel („Shared Secret“) für diesen VPN-Account. Dieser Wert ist nur vorhanden, wenn „AuthenticationMethod=SharedSecret“ ist. Dieser Wert wird für L2TP und Cisco IPSec verwendet.
PayloadCertificateUUID	Zeichenkette. Dies ist die UUID des Zertifikats für die Anmeldedaten des Accounts. Dieser Wert ist nur vorhanden, wenn „AuthenticationMethod=Certificate“ ist. Dieser Wert wird für Cisco IPSec verwendet.
PromptForVPNPIN	Boolesch. Dieser Wert gibt an, ob beim Verbindungsaufbau eine PIN angefordert wird. Dieser Wert wird für Cisco IPSec verwendet.

Payload-Segment „Wi-Fi“

Das Payload-Segment „Wi-Fi“ wird vom PayloadType-Wert „com.apple.wifi.managed“ bestimmt. Dies beschreibt Version 0 des Werts „PayloadVersion“. Zusätzlich zu den Einstellungen, die für alle Payload-Typen gleichermaßen gelten, definiert das Payload-Segment die folgenden Schlüssel.

Schlüssel	Wert
SSID_STR	Zeichenkette. Dies ist die SSID des zu verwendenden Wi-Fi-Netzwerks.
HIDDEN_NETWORK	Boolesch. Neben der SSID verwendet das Gerät Informationen wie Broadcast- oder Verschlüsselungstyp, um ein Netzwerk zu identifizieren. Standardmäßig wird davon ausgegangen, dass es sich bei allen konfigurierten Netzwerken um offene oder Broadcast-Netzwerke handelt. Zur Angabe eines versteckten Netzwerks müssen Sie einen booleschen Wert für den Schlüssel „HIDDEN_NETWORK“ hinzufügen.
EncryptionType	Zeichenkette. Die möglichen Werte für „EncryptionType“ sind „WEP“, „WPA“ oder „Any“. „WPA“ entspricht WPA und WPA2 und gilt für beide Verschlüsselungstypen. Vergewissern Sie sich, dass diese Werte genau zu den Leistungsmerkmalen des Netzwerkzugriffspunkts passen. Verwenden Sie den Wert „Any“, wenn Sie sich hinsichtlich des Verschlüsselungstyps unsicher sind oder möchten, dass er für alle Verschlüsselungstypen gilt.
Kennwort	Zeichenkette, optional. Ist kein Kennwort vorhanden, wird dadurch nicht verhindert, dass das Netzwerk zu der Liste der bekannten Netzwerke hinzugefügt wird. Beim Zugriff auf das Netzwerk wird der Benutzer schließlich aufgefordert, das Kennwort anzugeben.

Für 802.1X-Unternehmensnetzwerke muss das Funktionsverzeichnis des Schlüssels „EAPClientConfiguration“ angegeben werden.

Funktionsverzeichnis des Schlüssels „EAPClientConfiguration“

Neben den standardmäßigen Verschlüsselungstypen kann über den Schlüssel „EAPClientConfiguration“ ein Unternehmensprofil für ein bestimmtes Netzwerk festgelegt werden. Ist er vorhanden, ist sein Wert ein Funktionsverzeichnis mit den folgenden Schlüsseln.

Schlüssel	Wert
UserName	Zeichenkette, optional. Sofern Sie nicht den genauen Benutzernamen kennen, wird diese Eigenschaft in einer importierten Konfiguration nicht angezeigt. Benutzer können diese Informationen bei der Anmeldung eingeben.
AcceptEAPTypes	Datenfeld mit Ganzzahlen. Die folgenden EAP-Typen werden akzeptiert: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
PayloadCertificateAnchorUUID	Datenfeld mit Zeichenketten, optional. Identifiziert die Zertifikate, die für diese Anmeldung als vertrauenswürdig gelten. Jeder Eintrag muss die UUID des Payload-Segments des Zertifikats enthalten. Verwenden Sie diesen Schlüssel, um die Nachfrage des Geräts beim Benutzer zu verhindern, wenn die aufgelisteten Zertifikate als vertrauenswürdig gelten. Die dynamische Einstufung als vertrauenswürdig (das Dialogfenster des Zertifikats) ist deaktiviert, wenn diese Eigenschaft angegeben ist, es sei denn, „TLSAllowTrustExceptions“ ist ebenfalls mit dem Wert TRUE (wahr) angegeben.
TLSTrustedServerNames	Datenfeld mit Zeichenkettenwerten, optional. Hierbei handelt es sich um die Liste allgemeiner Namen für Serverzertifikate, die akzeptiert werden. Sie können bei der Angabe des Namens Platzhalterzeichen verwenden (z. B.: wpa.*.beispiel.com). Präsentiert ein Server ein Zertifikat, das nicht in der Liste enthalten ist, gilt dieses Zertifikat nicht als vertrauenswürdig. Die Eigenschaft wird alleine oder zusammen mit „TLSTrustedCertificates“ verwendet und ermöglicht die genaue Auswahl der Zertifikate, die für ein bestimmtes Netzwerk als vertrauenswürdig gelten sollen. Damit kann vermieden werden, dass Zertifikate dynamisch als vertrauenswürdig eingestuft werden. Die dynamische Einstufung als vertrauenswürdig (das Dialogfenster des Zertifikats) ist deaktiviert, wenn diese Eigenschaft angegeben ist, es sei denn, „TLSAllowTrustExceptions“ ist ebenfalls mit dem Wert TRUE (wahr) angegeben.

Schlüssel	Wert
TLSAllowTrustExceptions	Boolesch, optional. Dieser Wert ermöglicht bzw. verhindert die dynamische Einstufung eines Zertifikats durch einen Benutzer als vertrauenswürdig. Diese dynamische Einstufung erfolgt über das Dialogfenster für Zertifikate, das angezeigt wird, wenn ein Zertifikat nicht als vertrauenswürdig gilt. Beim Wert „FALSE“ schlägt die Anmeldung fehl, wenn das Zertifikat nicht bereits als vertrauenswürdig gilt. Vgl. „PayloadCertificateAnchorUUID“ und „TLSTrustedNames“ oben. Der Standardwert dieser Eigenschaft ist „TRUE“, es sei denn, „PayloadCertificateAnchorUUID“ oder „TLSTrustedServerNames“ wird angegeben. In diesem Fall ist der Standardwert „FALSE“.
TTLSInnerAuthentication	Zeichenkette, optional. Hierbei handelt es sich um die interne Identifizierung des TTLS-Moduls. Der Standardwert lautet „MSCHAPv2“. Mögliche Werte sind „PAP“, „CHAP“, „MSCHAP“ und „MSCHAPv2“.
OuterIdentity	Zeichenkette, optional. Dieser Schlüssel ist nur für TTLS, PEAP und EAP-FAST relevant. Hiermit kann der Benutzer seine Identität verbergen. Der richtige Name des Benutzers wird nur innerhalb des verschlüsselten Tunnels angezeigt. Die Identität könnte zum Beispiel auf „anonymous“, „anon“ oder „anon@unternehmen.net“ eingestellt werden. Dadurch kann die Sicherheit erhöht werden, da ein Angreifer den Namen des angemeldeten Benutzers nicht in Klartext lesen kann.

Unterstützung für EAP-Fast

Das Modul „EAP-FAST“ verwendet die folgenden Eigenschaften im Funktionsverzeichnis „EAPClientConfiguration“.

Schlüssel	Wert
EAPFASTUsePAC	Boolesch, optional.
EAPFASTProvisionPAC	Boolesch, optional.
EAPFASTProvisionPACAnonymously	Boolesch, optional.

Diese Schlüssel sind hierarchisch aufgebaut: Bei der Festlegung „EAPFASTUsePAC=FALSE“ werden die anderen beiden Eigenschaften nicht berücksichtigt. Bei der Festlegung „EAPFASTProvisionPAC=FALSE“ wird „EAPFASTProvisionPACAnonymously“ nicht berücksichtigt.

Bei der Festlegung „EAPFASTUsePAC=FALSE“ verläuft die Identifizierung sehr ähnlich wie für PEAP oder TTLS: der Server bestätigt seine Identität jedes Mal mithilfe eines Zertifikats.

Bei der Festlegung „EAPFASTUsePAC=TRUE“ wird ein vorhandenes PAC-Element verwendet. Die einzige Möglichkeit, derzeit ein PAC-Element auf das Gerät zu übertragen, besteht darin, die PAC-Bereitstellung zuzulassen. Sie müssen daher „EAPFASTProvisionPAC“ und gegebenenfalls auch „EAPFASTProvisionPACAnonymously“ aktivieren. “EAPFASTProvisionPACAnonymously“ hat einen Nachteil in Bezug auf die Sicherheit: der Server wird nicht identifiziert, sodass Verbindungen anfällig für MITM-Angriffe (Man-in-the-Middle) sind.

Zertifikate

Wie bei VPN-Konfigurationen kann die Konfiguration einer Zertifikatsidentität einer Wi-Fi-Konfiguration zugeordnet werden. Das ist bei der Definition von Anmeldedaten für ein sicheres Unternehmensnetzwerk von Nutzen. Sie können eine Identität zuordnen, indem Sie deren Payload-UUID über den Schlüssel „PayloadCertificateUUID“ angeben.

Schlüssel	Wert
PayloadCertificateUUID	Zeichenkette. Dies ist die UUID des Payload-Segments des Zertifikats zur Verwendung als Anmeldeinformation.

Muster für Konfigurationsprofile

Im Folgenden finden Sie Muster für Profile, die die drahtlose Registrierung und Konfiguration erläutern. Es handelt sich dabei um Auszüge und Ihre Anforderungen werden sich von den Beispielen unterscheiden. Hilfe zur Syntax finden Sie in den Details weiter vorne in diesem Kapitel. Beschreibungen der einzelnen Phasen finden Sie unter „Drahtlose Registrierung und Konfiguration“ auf Seite 25.

Muster für Phase 1 – Antwort des Servers

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https://profileserver.example.com/iphone</string>
        <key>DeviceAttributes</key>
        <array>
                <string>UDID</string>
  <string>IMEI</string>
  <string>ICCID</string>
  <string>VERSION</string>
  <string>PRODUCT</string>
        </array>
    <key>Challenge</key>
```

```
     <string>optional challenge</string>
     ODER
     <data>base64-encoded</data>
    </dict>
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string>Profile Service</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>fdb376e5-b5bb-4d8c-829e-e90865f990c9</string>
    <key>PayloadIdentifier</key>
    <string>com.example.mobileconfig.profile-service</string>
    <key>PayloadDescription</key>
    <string>Enter device into the Example Inc encrypted profile service</
     string>
    <key>PayloadType</key>
     <string>Profile Service</string>
</dict>
</plist>
```

Muster für Phase 2 – Antwort des Geräts

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
    <key>Challenge</key>
ENTWEDER:
    <string>String</string>
ODER:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

Muster für Phase 3 – Antwort des Servers mit SCEP-Spezifikationen

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadUUID</key>
  <string>Ignored</string>
  <key>PayloadType</key>
  <string>Configuration</string>
  <key>PayloadIdentifier</key>
  <string>Ignored</string>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadContent</key>
      <dict>
        <key>URL</key>
        <string>https://scep.example.com/scep</string>
        <key>Name</key>
        <string>EnrollmentCAInstance</string>
        <key>Subject</key>
        <array>
          <array>
            <array>
              <string>O</string>
              <string>Example, Inc.</string>
            </array>
          </array>
          <array>
            <array>
              <string>CN</string>
              <string>User Device Cert</string>
            </array>
          </array>
        </array>
        <key>Challenge</key>
        <string>...</string>
        <key>Keysize</key>
        <integer>1024</integer>
        <key>Key Type</key>
        <string>RSA</string>
        <key>Key Usage</key>
        <integer>5</integer>
      </dict>
      <key>PayloadDescription</key>
      <string>Provides device encryption identity</string>
      <key>PayloadUUID</key>
      <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
      <key>PayloadType</key>
```

```
        <string>com.apple.security.scep</string>
        <key>PayloadDisplayName</key>
        <string>Encryption Identity</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadOrganization</key>
        <string>Example, Inc.</string>
        <key>PayloadIdentifier</key>
        <string>com.example.profileservice.scep</string>
      </dict>
    </array>
  </dict>
</plist>
```

Muster für Phase 4 – Antwort des Geräts

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
</dict>
</plist>
```

Beispielskripte

In diesem Anhang finden Sie Beispielskripte für iPhone OS-Implementierungsaufgaben.

Die Skripte in diesem Abschnitt sollten an Ihre Anforderungen und Konfigurationen angepasst werden.

Beispielskript C# für das iPhone-Konfigurationsprogramm

Dieses Beispielskript zeigt die Erstellung von Konfigurationsdateien mit dem iPhone-Konfigurationsprogramm für Windows.

```
using System;
using Com.Apple.iPCUScripting;

public class TestScript : IScript
  {
  private IApplication _host;

  public TestScript()
     {
     }

  public void main(IApplication inHost)
     {
     _host = inHost;

     string msg = string.Format("# of config profiles : {0}", _host.Configu-
     rationProfiles.Count);
     Console.WriteLine(msg);

     IConfigurationProfile profile = _host.AddConfigurationProfile();
     profile.Name = "Profile Via Script";
     profile.Identifier = "com.example.configviascript";
     profile.Organization = "Example Org";
     profile.Description = "This is a configuration profile created via the
     new scripting feature in iPCU";

     // passcode
     IPasscodePayload passcodePayload = profile.AddPasscodePayload();
```

```
    passcodePayload.PasscodeRequired = true;
    passcodePayload.AllowSimple = true;

    // restrictions
    IRestrictionsPayload restrictionsPayload = profile.AddRestrictionsPay-
    load();
    restrictionsPayload.AllowYouTube = false;

    // wi-fi
    IWiFiPayload wifiPayload = profile.AddWiFiPayload();
    wifiPayload.ServiceSetIdentifier = "Example Wi-Fi";
    wifiPayload.EncryptionType = WirelessEncryptionType.WPA;
    wifiPayload.Password = "password";

    wifiPayload = profile.AddWiFiPayload();
    profile.RemoveWiFiPayload(wifiPayload);

    // vpn
    IVPNPayload vpnPayload = profile.AddVPNPayload();
    vpnPayload.ConnectionName = "Example VPN Connection";

    vpnPayload = profile.AddVPNPayload();
    profile.RemoveVPNPayload(vpnPayload);

    // email
    IEmailPayload emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 1 Via Scripting";

    emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 2 Via Scripting";

    // exchange
    IExchangePayload exchangePayload = profile.AddExchangePayload();
    exchangePayload.AccountName = "ExchangePayloadAccount";

    // ldap
    ILDAPPayload ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 1 Via Scripting";

    ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 2 Via Scripting";

    // webclip
    IWebClipPayload wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 1 Via Scripting";

    wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 2 Via Scripting";

    }
}
```

AppleScript-Beispielskript für das iPhone-Konfigurationsprogramm

Dieses Beispielskript zeigt die Erstellung von Konfigurationsdateien mit dem iPhone-Konfigurationsprogramm für Mac OS X.

```
tell application "iPhone Configuration Utility"
  log (count of every configuration profile)
  set theProfile to make new configuration profile with properties {dis-
     played name:"Profile Via Script", profile identifier:"com.example.con-
     figviascript", organization:"Example Org.", account description:"This
     is a configuration profile created via AppleScript"}
  tell theProfile
     make new passcode payload with properties {passcode required:true, sim-
     ple value allowed:true}
     make new restrictions payload with properties {YouTube allowed:false}
     make new WiFi payload with properties {service set identifier:"Example
     Wi-Fi", security type:WPA, password:"password"}
     set theWiFiPayload to make new WiFi payload
     delete theWiFiPayload
     make new VPN payload with properties {connection name:"Example VPN Con-
     nection"}
     set theVPNPayload to make new VPN payload
     delete theVPNPayload
     make new email payload with properties {account description:"Email
     Account 1 Via Scripting"}
     make new email payload with properties {account description:"Email
     Account 2 Via Scripting"}
     make new Exchange ActiveSync payload with properties {account
     name:"ExchangePayloadAccount"}
     make new LDAP payload with properties {account description:"LDAP
     Account 1 Via Scripting"}
     make new LDAP payload with properties {account description:"LDAP
     Account 2 Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 1
     Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 2
     Via Scripting"}
  end tell
end tell
```