iPhone OS
Implementatie-handleiding voor bedrijven

Tweede editie, voor versie 3.2 of hoger

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

Gelijktijdig uitgebracht in de Verenigde Staten en Canada.

N019-1835/2010-04

Inhoudsopgave

Voorwoord 6 **De iPhone in een bedrijfsomgeving**
6 Nieuwe functies voor bedrijven in iPhone OS 3.0 en hoger
7 Systeemvereisten
8 Microsoft Exchange ActiveSync
11 VPN
11 Netwerkbeveiliging
12 Certificaten en identiteiten
13 E-mailaccounts
13 LDAP-servers
13 CalDAV-servers
14 Meer informatie

Hoofdstuk 1 15 **De iPhone en iPod touch implementeren**
16 Apparaten activeren
17 Toegang tot netwerkvoorzieningen en bedrijfsgegevens voorbereiden
22 Kiezen welke beleidsinstellingen voor toegangscodes u voor de apparaten wilt gebruiken
22 Apparaten configureren
24 Over-the-air-aanmeldingen en -configuratie
29 Meer informatie

Hoofdstuk 2 30 **Configuratieprofielen aanmaken en implementeren**
31 iPhone-configuratieprogramma
32 Configuratieprofielen aanmaken
44 Configuratieprofielen wijzigen
44 Voorzieningenprofielen en programma's installeren
44 Configuratieprofielen installeren
48 Configuratieprofielen verwijderen en bijwerken

Hoofdstuk 3 50 **Apparaten handmatig configureren**
50 VPN-instellingen
54 Wi-Fi-instellingen
55 Exchange-instellingen
60 Identiteiten en rootcertificaten installeren

61 Extra e-mailaccounts
61 Profielen bijwerken en verwijderen
61 Meer informatie

Hoofdstuk 4 63 **iTunes implementeren**
63 iTunes installeren
65 Apparaten snel activeren met iTunes
66 Beperkingen instellen voor iTunes
68 Een reservekopie maken van een apparaat met iTunes

Hoofdstuk 5 70 **Programma's implementeren**
70 Aanmelden voor het ontwikkelen van programma's
71 Programma's ondertekenen
71 Het voorzieningenprofiel voor distributie aanmaken
71 Voorzieningenprofielen installeren via iTunes
72 Voorzieningenprofielen installeren met iPhone-configuratieprogramma
72 Programma's installeren via iTunes
73 Programma's installeren met iPhone-configuratieprogramma
73 Werken met bedrijfsprogramma's
73 Een bedrijfsprogramma uitschakelen
73 Meer informatie

Bijlage A 74 **Configuratie van de Cisco VPN-server**
74 Ondersteunde Cisco-platforms
74 Methoden voor identiteitscontrole
75 Identiteitscontrolegroepen
75 Certificaten
76 IPSec-instellingen
76 Overige ondersteunde functies

Bijlage B 78 **De structuur van configuratieprofielen**
78 Hoofdniveau
80 Inhoud van de payload
81 Profile Removal Password Payload
81 De payload 'Toegangscode'
83 De payload 'E-mail'
84 De payload 'Webknipsels'
85 De payload 'Beperkingen'
86 De payload 'LDAP'
87 De payload 'CalDAV'
87 De payload 'Agenda's met abonnement'
88 De payload 'SCEP'
89 De payload 'APN'
89 De payload 'Exchange'

90 De payload 'VPN'
92 De payload 'Wi-Fi'
95 Voorbeeldconfiguratieprofielen

Bijlage C 99 **Voorbeeldscripts**

De iPhone in een bedrijfsomgeving

Deze handleiding bevat informatie over het integreren van de iPhone, iPod touch en iPad in uw bedrijfsomgeving.

Deze handleiding is bestemd voor systeembeheerders en bevat informatie over het implementeren en ondersteunen van de iPhone, iPod touch en iPad in een bedrijfsomgeving.

Nieuwe functies voor bedrijven in iPhone OS 3.0 en hoger

iPhone OS 3.x bevat verschillende verbeteringen. Een overzicht van de verbeteringen die van toepassing zijn voor zakelijke gebruikers:

- Ondersteuning voor draadloze synchronisatie van CalDAV-agenda's
- LDAP-serverondersteuning voor het opzoeken van contactpersonen in e-mailberichten, adresboek en sms-berichten
- Codering en vergrendeling van configuratieprofielen aan een apparaat, zodat het profiel alleen kan worden verwijderd als het beheerderswachtwoord wordt opgegeven
- Met iPhone-configuratieprogramma gecodeerde configuratieprofielen rechtstreeks toevoegen aan en verwijderen van apparaten die via USB met uw computer zijn verbonden
- Ondersteuning voor OCSP (Online Certificate Status Protocol) voor de intrekking van certificaten
- Ondersteuning voor op certificaten gebaseerde VPN-verbindingen op verzoek
- Ondersteuning voor VPN-proxyconfiguratie via een configuratieprofiel en VPN-servers
- Via Microsoft Exchange personen uitnodigen voor vergaderingen (Microsoft Exchange 2007-gebruikers kunnen ook de antwoordstatus bekijken)
- Ondersteuning voor identiteitscontrole op basis van certificaten voor Exchange ActiveSync-clients
- Ondersteuning voor extra EAS-beleidsinstellingen, in combinatie met EAS-protocol 12.1

- Extra apparaatbeperkingen, waaronder het uitschakelen van de camera, de mogelijkheid om op te geven hoe lang een apparaat ontgrendeld kan blijven en de mogelijkheid om gebruikers te beletten een schermafbeelding te maken
- De mogelijkheid om te zoeken in lokale e-mailberichten en agenda-activiteiten (in IMAP, MobileMe en Exchange 2007 kan ook worden gezocht in e-mailberichten die op de server blijven staan)
- Extra postmappen toewijzen voor de levering van push-e-mail
- Met behulp van een configuratieprofiel APN-proxyinstellingen opgeven
- Webknipsels installeren met behulp van een configuratieprofiel
- Ondersteuning voor 802.1x EAP-SIM
- Over-the-air uitvoeren van identiteitscontroles en aanmelden van apparaten via een SCEP-server (Simple Certificate Enrollment Protocol)
- Bewaren van gecodeerde reservekopieën van gegevens op apparaten in iTunes
- Ondersteuning in iPhone-configuratieprogramma voor het aanmaken van profielen via een script
- Ondersteuning in iPhone-configuratieprogramma 2.2 voor iPad, iPhone en iPod touch (hiervoor is Mac OS X v10.6 Snow Leopard vereist; Windows 7 wordt tevens ondersteund)

Systeemvereisten

In dit gedeelte wordt een overzicht gegeven van de systeemvereisten en van de verschillende onderdelen die beschikbaar zijn voor de integratie van de iPhone, iPod touch en iPad in uw bedrijfsomgeving.

iPhone en iPod touch

Op de iPhone- en iPod touch-apparaten die u in uw bedrijfsnetwerk gebruikt, moet iPhone OS 3.1.x zijn geïnstalleerd.

iPad

Op de iPad moet iPhone OS 3.2.x zijn geïnstalleerd.

iTunes

Voor de configuratie van de apparaten is iTunes 9.1 of hoger vereist. iTunes is tevens vereist voor de installatie van software-updates op de iPhone, iPod touch en iPad. Bovendien hebt u iTunes nodig voor de installatie van programma's en de synchronisatie van muziek, video's, notities of ander materiaal met een Mac of pc.

Om iTunes te kunnen gebruiken, hebt u een Mac of pc met een USB 2.0-poort nodig die voldoet aan de minimumvereisten die op de iTunes-website worden vermeld. Ga naar www.apple.com/nl/itunes/download/.

iPhone-configuratieprogramma

Met iPhone-configuratieprogramma kunt u configuratieprofielen aanmaken, coderen en installeren, voorzieningenprofielen en bevoegde programma's volgen en installeren, en apparaatgegevens vastleggen, zoals consolelogbestanden.

Voor iPhone-configuratieprogramma gelden de volgende vereisten:

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

iPhone-configuratieprogramma werkt in de 32-bits-modus in 64-bits-versies van Windows.

U kunt het installatieprogramma voor .Net Framework 3.5 Service Pack 1 downloaden vanaf:
http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

Met het programma kunt u een Outlook-bericht aanmaken en hieraan een configuratieprofiel als bijlage toevoegen. Daarnaast kunt u de namen en e-mailadressen van gebruikers uit het adresboek van uw desktopcomputer toewijzen aan apparaten die u aan het programma hebt gekoppeld. Voor beide functies is Outlook vereist; u kunt deze functies niet gebruiken als u met Outlook Express werkt. Om deze functies op Windows XP-computers te gebruiken, dient u mogelijk 2007 Microsoft Office System Update: Redistributable Primary Interop Assemblies te installeren. Deze update is noodzakelijk als Outlook al was geïnstalleerd voordat .NET Framework 3.5 Service Pack 1 is geïnstalleerd.

Het installatieprogramma voor Primary Interop Assemblies is beschikbaar op:
http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

De iPhone, iPod touch en iPad ondersteunen de volgende versies van Microsoft Exchange:

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

Voor ondersteuning van beleidsinstellingen en functies voor Exchange 2007 is Service Pack 1 vereist.

Ondersteunde Exchange ActiveSync-beleidsinstellingen

De volgende Exchange-beleidsinstellingen worden ondersteund:

- Enforce password on device
- Minimum password length
- Maximum failed password attempts
- Require both numbers and letters
- Inactivity time in minutes

Daarnaast worden de volgende Exchange 2007-beleidsinstellingen ondersteund:

- Allow or prohibit simple password
- Password expiration
- Password history
- Policy refresh interval
- Minimum number of complex characters in password
- Require manual syncing while roaming
- Allow camera
- Require device encryption

Raadpleeg de documentatie bij Exchange ActiveSync voor een beschrijving van de beleidsinstellingen.

Het Exchange-beleid dat apparaatcodering (RequireDeviceEncryption) voorschrijft, wordt ondersteund op de iPhone 3GS, iPod touch (modellen van najaar 2009 met minimaal 32 GB) en op de iPad. De iPhone, iPhone 3G en andere iPod touch-modellen bieden geen ondersteuning voor apparaatcodering; vanaf die apparaten is het niet mogelijk verbinding te maken met een Exchange Server waarbij apparaatcodering is vereist.

Wanneer u het beleid 'Require Both Numbers and Letters' inschakelt op Exchange 2003 of het beleid 'Require Alphanumeric Password' op Exchange 2007, moet de gebruiker een toegangscode voor het apparaat invoeren die ten minste één complex teken bevat.

De waarde die door het inactiviteitsbeleid ('MaxInactivityTimeDeviceLock' of 'AEFrequencyValue') is opgegeven, wordt gebruikt om de maximumwaarde in te stellen die gebruikers kunnen selecteren bij zowel 'Instellingen' > 'Algemeen' > 'Automatisch slot' als 'Instellingen' > 'Algemeen' > 'Codeslot' > 'Vraag om code'.

Remote Wipe

U kunt de inhoud van een iPhone, iPod touch of iPad op afstand wissen (met de functie 'Remote Wipe'). Hierbij worden alle configuratiegegevens en andere gegevens van het apparaat verwijderd. Het apparaat wordt op een veilige manier gewist en de fabrieksinstellingen worden hersteld.

Belangrijk: Wanneer een iPhone of iPhone 3G wordt gewist, worden de gegevens op het apparaat overschreven; de wisbewerking kan voor elke 8 GB aan apparaatcapaciteit één uur in beslag nemen. Sluit het apparaat daarom aan op een stopcontact voordat u de inhoud van het apparaat wist. Als het apparaat wordt uitgeschakeld omdat de batterij bijna leeg is, kunt u het apparaat op een stopcontact aansluiten om het wissen te hervatten. Op iPhone 3GS en iPad vindt het wissen onmiddellijk plaats en wordt de coderingssleutel voor de gegevens (die zijn gecodeerd met 256-bits-AES-codering) verwijderd.

Met Exchange Server 2007 kunt u een Remote Wipe uitvoeren via de Exchange Management Console, Outlook Web Access of Exchange ActiveSync Mobile Administration Web Tool.

Met Exchange Server 2003 kunt u een Remote Wipe uitvoeren via Exchange ActiveSync Mobile Administration Web Tool.

Gebruikers kunnen een apparaat ook wissen door achtereenvolgens te tikken op 'Instellingen' > Algemeen' > 'Stel opnieuw in' > 'Wis alle inhoud en instellingen'. Het is ook mogelijk in de configuratie van apparaten te definiëren dat er automatisch een wisbewerking wordt geïnitieerd nadat er een bepaald aantal keer een onjuiste toegangscode is ingevoerd.

Als u een apparaat herstelt dat is gewist omdat het kwijt was, gebruikt u iTunes om het apparaat te herstellen aan de hand van de laatste back-up van het apparaat.

Microsoft Direct Push

De Exchange-server levert automatisch e-mailberichten, gegevens van contactpersonen en agenda-activiteiten aan de iPhone en iPad Wi-Fi + 3G als een mobiel telefoonnetwerk of Wi-Fi-datanetwerk beschikbaar is. Aangezien de iPod touch en iPad Wi-Fi geen verbinding via een mobiel telefoonnetwerk kunnen maken, moeten deze apparaten geactiveerd zijn en verbinding hebben met een Wi-Fi-netwerk om pushberichten te kunnen ontvangen.

Microsoft Exchange Autodiscovery

Er is ondersteuning voor de Autodiscover-voorziening van Exchange Server 2007. Wanneer u een apparaat handmatig configureert, bepaalt de Autodiscover-voorziening op basis van uw e-mailadres en wachtwoord automatisch wat de juiste gegevens voor de Exchange-server zijn. Voor informatie over het inschakelen van de Autodiscover-voorziening gaat u naar: http://technet.microsoft.com/en-us/library/cc539114.aspx

Microsoft Exchange Global Address List

De iPhone, iPod touch en iPad halen gegevens van contactpersonen op uit de algemene adreslijst op de Exchange-server van het bedrijf. U kunt deze adreslijst raadplegen wanneer u contactpersonen zoekt. Ook wordt de lijst automatisch gebruikt voor het aanvullen van e-mailadressen die u opgeeft.

Extra ondersteunde functies van Exchange ActiveSync

Naast de functies en voorzieningen die al zijn beschreven, biedt iPhone OS ondersteuning voor het volgende:

- Uitnodigingen voor agenda-activiteiten aanmaken (met Microsoft Exchange 2007 kunt u ook de status van antwoorden op uw uitnodigingen bekijken)
- De status 'Vrij', 'Bezig', 'Onbeslist' of 'Niet op kantoor' instellen voor uw agenda-activiteiten
- E-mailberichten op de server zoeken (hiervoor is Microsoft Exchange 2007 vereist)
- Identiteitscontrole op basis van certificaten uitvoeren voor Exchange ActiveSync-clients

Niet-ondersteunde functies van Exchange ActiveSync

Bepaalde functies van Exchange worden niet ondersteund, zoals:

- Mappenbeheer
- Documenten openen op Sharepoint-servers via een koppeling in een e-mail
- Taken synchroniseren
- Een bericht instellen voor een automatisch antwoord bij afwezigheid
- Berichten markeren waaraan u nog aandacht moet besteden

VPN

iPhone OS werkt met VPN-servers die de volgende protocollen en methoden voor identiteitscontrole ondersteunen:

- L2TP/IPSec met identiteitscontrole van gebruikers via een MS-CHAPV2-wachtwoord, RSA SecurID of CryptoCard, en met identiteitscontrole van apparaten via een gedeeld geheim
- PPTP met identiteitscontrole van gebruikers via een MS-CHAPV2-wachtwoord, RSA SecurID of CryptoCard
- Cisco IPSec met identiteitscontrole van gebruikers via een wachtwoord, RSA SecurID of CryptoCard, en met identiteitscontrole van apparaten via een gedeeld geheim en certificaten (Zie bijlage A voor compatibele Cisco VPN-servers en aanbevelingen voor configuraties.)

Cisco IPSec met identiteitscontrole op basis van certificaten biedt ondersteuning voor VPN op aanvraag voor domeinen die u tijdens de configuratie opgeeft. Zie “VPN” op pagina 38 voor meer informatie.

Netwerkbeveiliging

iPhone OS ondersteunt de volgende beveiligingsstandaarden voor draadloze 802.11i-netwerkverbindingen zoals gedefinieerd door de Wi-Fi Alliance:

- WEP
- WPA - persoonlijk
- WPA - bedrijfsniveau
- WPA2 - persoonlijk
- WPA2 - bedrijfsniveau

Daarnaast worden de volgende 802.1X-methoden voor identiteitscontrole ondersteund voor WPA- en WPA2-netwerken op bedrijfsniveau:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP versie 0, PEAP versie 1
- LEAP

Certificaten en identiteiten

De iPhone, iPod touch en iPad kunnen gebruikmaken van X.509-certificaten met RSA-sleutels. De bestandsextensies .cer, .crt en .der worden herkend. Er worden bepaalde ketenevaluaties uitgevoerd door Safari, Mail, VPN en andere programma's.

U kunt gebruikmaken van P12-bestanden (PKCS #12-standaard) met precies één identiteit. De bestandsextensies .p12 en .pfx worden herkend. Nadat een identiteit is geïnstalleerd, wordt de gebruiker om de wachtzin gevraagd waarmee de identiteit is beveiligd.

Certificaten die nodig zijn bij de koppeling tussen een certificaatketen en een vertrouwd rootcertificaat kunnen handmatig worden geïnstalleerd of met behulp van een configuratieprofiel. Het is niet nodig om rootcertificaten toe te voegen die door Apple bij het apparaat zijn geleverd. Raadpleeg het Apple Support-artikel op http://support.apple.com/kb/HT3580?viewlocale=nl_NL voor een lijst met vooraf geïnstalleerde systeemroots.

Certificaten kunnen veilig over-the-air worden geïnstalleerd via SCEP. Zie “Overzicht van het aanmeldings- en configuratieproces met identiteitscontrole” op pagina 24 voor meer informatie.

E-mailaccounts

De iPhone, iPod touch en iPad ondersteunen standaard IMAP4- en POP3-e-mailvoorzieningen voor diverse serverplatforms waaronder Windows, UNIX, Linux en Mac OS X. U kunt ook IMAP gebruiken om e-mail te benaderen van Exchange-accounts bovenop de Exchange-account die u met "direct push" gebruikt.

Bij een zoekactie in e-mailberichten kunnen gebruikers de zoekactie voortzetten op de mailserver. Deze functie werkt in combinatie met Microsoft Exchange Server 2007 en de meeste op IMAP-gebaseerde accounts.

De e-mailaccountgegevens van de gebruiker, waaronder de gebruikers-ID en het wachtwoord voor Exchange, worden veilig op het apparaat bewaard.

LDAP-servers

Met de iPhone, iPod touch en iPad worden de contactgegevens opgehaald uit de bedrijfsadreslijsten van de LDAPv3-server van uw bedrijf. U kunt deze adreslijst raadplegen wanneer u contactpersonen zoekt. Ook wordt de lijst automatisch gebruikt voor het aanvullen van e-mailadressen die u opgeeft.

CalDAV-servers

Op de iPhone, iPod touch en iPad worden agendagegevens gesynchroniseerd met de CalDAV-server van uw bedrijf. Wijzigingen in de agenda worden regelmatig bijgewerkt tussen het apparaat en de server.

Daarnaast kunt u een abonnement nemen op alleen-lezenagenda's die zijn gepubliceerd, zoals agenda's met vakantiedagen of agenda's met de planning van een collega.

Het aanmaken en verzenden van nieuwe agenda-uitnodigingen vanaf een apparaat wordt niet ondersteund voor CalDAV-accounts.

Meer informatie

Naast deze handleiding bieden de volgende publicaties en websites handige informatie:

- De webpagina 'iPhone voor zakelijk gebruik' op www.apple.com/nl/iphone/enterprise
- De webpagina 'iPad in het bedrijfsleven' op www.apple.com/nl/ipad/business/
- Een overzicht van Exchange op http://technet.microsoft.com/en-us/library/bb124558.aspx
- De webpagina 'Deploying Exchange ActiveSync' op http://technet.microsoft.com/en-us/library/aa995962.aspx
- Exchange 2003 Technical Documentation Library op http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx
- De webpagina 'Managing Exchange ActiveSync Security' op http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx
- De webpagina 'Wi-Fi for Enterprise' op www.wi-fi.org/enterprise.php
- De webpagina 'iPhone VPN Connectivity to Cisco Adaptive Security Appliances (ASA)' op www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html
- De *iPhone-gebruikershandleiding*, die u kunt downloaden via www.apple.com/nl/support/iphone/. Om de handleiding op de iPhone te bekijken, tikt u op de bladwijzer voor de iPhone-gebruikershandleiding in Safari of gaat u naar http://help.apple.com/iphone/.
- De iPhone-rondleiding op www.apple.com/nl/iphone/guidedtour
- De *iPod touch-gebruikershandleiding*, die u kunt downloaden via www.apple.com/nl/support/ipodtouch/. Om de handleiding op de iPod touch te bekijken, tikt u op de bladwijzer voor de iPod touch-gebruikershandleiding in Safari of gaat u naar http://help.apple.com/ipodtouch/.
- De iPod touch-rondleiding op www.apple.com/nl/ipodtouch/guidedtour
- De *iPad-gebruikershandleiding*, die u kunt downloaden via www.apple.com/nl/support/ipad. Om de handleiding op de iPad te bekijken, tikt u op de bladwijzer voor de iPad-gebruikershandleiding in Safari of gaat u naar http://help.apple.com/ipad/.
- De iPad-rondleiding op www.apple.com/ipad/guided-tours/

De iPhone en iPod touch implementeren

1

In dit hoofdstuk wordt uiteengezet hoe u de iPhone, iPod touch en iPad in uw bedrijfsomgeving implementeert.

De iPhone, iPod touch en iPad zijn zo ontworpen dat ze eenvoudig kunnen worden geïntegreerd in bedrijfsomgevingen met Microsoft Exchange 2003 en 2007, beveiligde draadloze 802.1X-netwerken en VPN's (Virtual Private Network) die gebruikmaken van Cisco IPSec. Zoals dat bij alle oplossingen voor bedrijfsomgevingen het geval is, zorgen een goede planning en begrip van de mogelijkheden ervoor dat de implementatie eenvoudiger en efficiënter verloopt voor u en uw gebruikers.

Bij de implementatie van de iPhone, iPod touch en iPad is het volgende van belang:

- Hoe worden de iPhone en de iPad (Wi-Fi + 3G-modellen) van uw bedrijf geactiveerd voor toegang tot een draadloos mobiel netwerk?
- Welke netwerkvoorzieningen, programma's en gegevens moeten toegankelijk zijn voor de gebruikers van uw bedrijfsomgeving?
- Welke beleidsinstellingen wilt u voor de apparaten opgeven om gevoelige bedrijfsinformatie te beschermen?
- Wilt u apparaten afzonderlijk handmatig configureren of een gestroomlijnd proces gebruiken om een groot aantal apparaten in één keer te configureren?

De specifieke kenmerken van uw bedrijfsomgeving, uw IT-beleid, uw telecomaanbieder en uw computer- en communicatievereisten zijn bepalend voor uw implementatiestrategie.

Apparaten activeren

Elke iPhone moet door uw telecomaanbieder zijn geactiveerd voordat het apparaat kan worden gebruikt om te bellen, gebeld te worden, sms-berichten te versturen of verbinding te maken met een mobiel datanetwerk. Neem contact op met uw telecomaanbieder als u meer wilt weten over de tarieven voor spraak- en dataverkeer en het activeren van de iPhone door consumenten en zakelijke gebruikers.

U of de gebruiker van de iPhone moet een simkaart in de iPhone installeren. Nadat de simkaart is geïnstalleerd, moet de iPhone op een computer met iTunes worden aangesloten om het activeringsproces te voltooien. Als de simkaart al is geactiveerd, is de iPhone direct klaar voor gebruik. Als de simkaart nog niet is geactiveerd, volgt u in iTunes de stapsgewijze instructies voor het activeringsproces.

De iPad moet verbonden zijn met een computer met iTunes om het apparaat te kunnen activeren. In de Verenigde Staten moet u zich voor het Wi-Fi + 3G-model van de iPad aanmelden en met behulp van uw iPad een AT&T-gegevensplan beheren (of annuleren). Tik op 'Instellingen' > 'Mobiele data' > 'Toon account'. De iPad wordt ontgrendeld, zodat u een aanbieder naar keuze kunt instellen. Neem contact op met uw aanbieder om een account aan te maken en een compatibele microsimkaart te bestellen. In de Verenigde Staten worden microsimkaarten die compatibel zijn met AT&T bij het Wi-Fi + 3G-model van de iPad meegeleverd.

Hoewel de iPod touch en de iPad Wi-Fi niet over een simkaart of telecomvoorzieningen beschikken, moeten deze ook op een computer met iTunes worden aangesloten om te worden geactiveerd.

Aangezien u het apparaat alleen met iTunes kunt activeren, moet u kiezen of u iTunes op de Mac of pc van alle gebruikers installeert, of dat u alle apparaten activeert met uw eigen exemplaar van iTunes.

Nadat het activeringsproces is afgerond, is iTunes niet meer noodzakelijk voor gebruik van de iPhone of iPod touch binnen uw bedrijfsomgeving. iTunes is echter wel vereist voor het synchroniseren van muziek, video's en de bladwijzers met een computer. iTunes is eveneens vereist voor het downloaden en installeren van software-updates en het installeren van uw bedrijfsprogramma's.

Zie Hoofdstuk 4 voor meer informatie over het activeren van apparaten en het gebruik van iTunes.

Toegang tot netwerkvoorzieningen en bedrijfsgegevens voorbereiden

De iPhone OS 3.x-software maakt het gebruik van beveiligde push-e-mail, pushcontactgegevens en pushagenda's mogelijk in combinatie met uw bestaande Microsoft Exchange Server 2003- of 2007-oplossing en biedt ondersteuning voor GAL (Global Address Lookup), wissen op afstand (Remote Wipe) en beleidsinstellingen voor het gebruik van toegangscodes. Bovendien kunnen gebruikers een beveiligde verbinding met bedrijfsgegevens en -apparatuur tot stand brengen via een draadloos WPA- of WPA2-netwerk met draadloze 802.1X-identiteitscontrole en/of via een VPN-netwerk met PPTP, LT2P over IPSec of Cisco IPSec.

Als uw bedrijf geen Microsoft Exchange gebruikt, kunnen uw gebruikers de iPhone of iPod touch toch gebruiken om e-mail draadloos te synchroniseren met de meeste standaard-POP- of IMAP-servers en -voorzieningen. En ze kunnen iTunes gebruiken om agenda-activiteiten en contactgegevens uit iCal en Adresboek in Mac OS X of Microsoft Outlook in Windows te synchroniseren. Voor draadloze toegang tot agenda's en adreslijsten worden CalDAV en LDAP ondersteund.

Zie de informatie in de volgende gedeelten bij de keuze van de netwerkvoorzieningen die u toegankelijk wilt maken voor gebruikers.

Microsoft Exchange

De iPhone kan rechtstreeks met Microsoft Exchange Server communiceren via Microsoft Exchange ActiveSync (EAS). Exchange ActiveSync onderhoudt een verbinding tussen Exchange Server en de iPhone of de iPad Wi-Fi + 3G waardoor het apparaat onmiddellijk wordt bijgewerkt als een nieuw e-mailbericht of een nieuwe uitnodiging voor een vergadering wordt ontvangen. Aangezien de iPod touch en de iPad Wi-Fi geen verbinding via een mobiel telecomnetwerk kunnen maken, moeten deze apparaten geactiveerd en verbonden zijn met een Wi-Fi-netwerk om pushberichten te kunnen ontvangen.

Als uw bedrijf gebruikmaakt van Exchange ActiveSync en Exchange Server 2003 of Exchange Server 2007, zijn alle noodzakelijke voorzieningen al aanwezig. Voor Exchange Server 2007 zorgt u ervoor dat de Client Access Role is geïnstalleerd. Voor Exchange Server 2003 zorgt u ervoor dat u Outlook Mobile Access (OMA) hebt ingeschakeld.

Raadpleeg de informatie in de volgende gedeelten als uw bedrijf al gebruikmaakt van Exchange Server, maar nog niet van Exchange ActiveSync.

Netwerkconfiguratie

- Zorg ervoor dat poort 443 in de firewall is geopend. Maakt uw bedrijf gebruik van Outlook Web Access, dan is poort 443 waarschijnlijk al geopend.

- Controleer of er een servercertificaat is geïnstalleerd op de Exchange-frontendserver en schakel alleen elementaire identiteitscontrole in de eigenschappen van de identiteitscontrolemethode in voor een SSL-verbinding met de Microsoft Server ActiveSync-directory van uw IIS.
- Als u een ISA-server (Microsoft Internet Security and Acceleration Server) gebruikt, controleert u of er een servercertificaat is geïnstalleerd en zorgt u dat inkomende verbindingen correct worden omgezet door de publieke DNS-server.
- Zorg ervoor dat de DNS-server van uw netwerk een enkelvoudig, extern routeerbaar adres teruggeeft aan de Exchange ActiveSync-server voor zowel intranet- als internetclients. Dit is noodzakelijk om ervoor te zorgen dat het apparaat hetzelfde IP-adres kan gebruiken om met de server te communiceren als beide typen verbindingen actief zijn.
- Als u een Microsoft ISA-server gebruikt, maakt u een web listener en een publicatieregel voor Exchange-webclienttoegang aan. Raadpleeg de documentatie van Microsoft voor meer informatie.
- Stel de time-out voor inactiviteit van alle firewalls en netwerkapparaten in op dertig minuten. Voor informatie over heartbeat- en time-out-intervallen raadpleegt u de documentatie bij Microsoft Exchange op http://technet.microsoft.com/en-us/library/cc182270.aspx.

Exchange-accounts configureren

- Schakel Exchange ActiveSync voor specifieke gebruikers of groepen in via de Active Directory-voorziening. Gebruikers en groepen zijn standaard ingeschakeld voor alle mobiele apparaten op organisatieniveau in Exchange Server 2003 en Exchange Server 2007. Als u Exchange Server 2007 gebruikt, vindt u meer informatie onder Recipient Configuration in de Exchange Management Console.
- Configureer de mobiele functies, beleidsinstellingen en de apparaatbeveiligingsinstellingen via de Exchange System Manager. In Exchange Server 2007 doet u dit via de Exchange Management Console.
- Download en installeer Microsoft Exchange ActiveSync Mobile Administration Web Tool. Deze tool is noodzakelijk om de gegevens op een apparaat op afstand te wissen. In Exchange Server 2007 kunnen gegevens ook op afstand worden gewist via Outlook Web Access of de Exchange Management Console.

Wi-Fi-bedrijfsnetwerken met WPA/WPA2

Dankzij ondersteuning voor WPA en WPA2 op bedrijfsniveau kunnen de iPhone, iPod touch en iPad veilig gebruikmaken van draadloze bedrijfsnetwerken. WPA/WPA2 op bedrijfsniveau maakt gebruik van AES 128-bits-codering, een beproefde coderingsmethode die ervoor zorgt dat bedrijfsgegevens goed zijn beveiligd.

Ondersteuning voor 802.1X-identiteitscontrole zorgt ervoor dat iPhone OS-apparaten in uiteenlopende RADIUS-serveromgevingen kunnen worden geïntegreerd. Verschillende methoden voor draadloze identiteitscontrole via 802.1X worden ondersteund, zoals EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 en LEAP.

WPA/WPA2-bedrijfsnetwerken configureren

- Controleer of de netwerkapparaten compatibel zijn en selecteer een type identiteitscontrole (EAP-type) dat door de iPhone, iPod touch en iPad wordt ondersteund. Zorg dat 802.1X is ingeschakeld op de server voor identiteitscontrole. Indien noodzakelijk installeert u een servercertificaat en kent u bevoegdheden voor netwerktoegang aan de gebruikers en groepen toe.
- Configureer de draadloze toegangspunten voor 802.1X-identiteitscontrole en geef de bijbehorende informatie over de RADIUS-server op.
- Test uw 802.1X-implementatie met een Mac of pc om te controleren of de RADIUS-identiteitscontrole juist is geconfigureerd.
- Als u van plan bent om gebruik te maken van identiteitscontrole op basis van certificaten, moet u ervoor zorgen dat uw publieke sleutel het gebruik van apparaat- en gebruikercertificaten via het bijbehorende sleuteldistributieproces ondersteunt.
- Controleer of de certificaatstructuur compatibel is met het apparaat en met uw server voor identiteitscontrole. Zie “Certificaten en identiteiten” op pagina 12 voor informatie over certificaten.

Virtual Private Networks

De iPhone, iPod touch en iPad bieden ondersteuning voor beveiligde toegang tot VPN-netwerken via Cisco IPSec, L2TP over IPSec en PPTP. Als uw organisatie gebruikmaakt van een van deze protocollen, hoeft u uw netwerk verder niet te configureren en hebt u geen programma's van andere fabrikanten nodig. U kunt de apparaten direct gebruiken in uw VPN-infrastructuur.

Cisco IPsec-implementaties kunnen gebruikmaken van identiteitscontrole op basis van veelgebruikte digitale X.509-certificaten. Als u met identiteitscontrole op basis van certificaten werkt, kunt u gebruikmaken van VPN op aanvraag, waarmee u kunt zorgen voor een naadloze en veilige draadloze toegang tot uw bedrijfsnetwerk.

iPhone OS biedt ondersteuning voor op tokens gebaseerde identiteitscontrole met twee factoren via RSA SecurID en CryptoCard. Gebruikers voeren hun pincode en hun, met een token gegenereerde, eenmalige wachtwoord in op het apparaat zelf tijdens het tot stand brengen van de VPN-verbinding. Zie bijlage A voor compatibele Cisco VPN-servers en aanbevelingen voor configuraties.

De iPhone, iPod touch en iPad bieden tevens ondersteuning voor identiteitscontrole op basis van gedeelde geheimen in Cisco IPSec- en L2TP/IPSec-implementaties en voor het gebruik van MS-CHAPv2 voor eenvoudige identiteitscontrole op basis van gebruikersnamen en wachtwoorden.

Automatische configuratie van de VPN-proxy (PAC en WPAD) wordt ook ondersteund, zodat u proxyserverinstellingen kunt opgeven voor toegang tot specifieke URL's.

Richtlijnen voor VPN-configuratie

- iPhone OS kan in de meeste bestaande VPN-netwerken worden geïntegreerd, waardoor de configuratie die noodzakelijk is om het apparaat toegang tot uw netwerk te geven tot een minimum beperkt blijft. U kunt de implementatie het best voorbereiden door te controleren of de bestaande VPN-protocollen en -methoden voor identiteitscontrole van uw bedrijf door de iPhone worden ondersteund.
- Zorg dat uw VPN-concentrators aan de standaarden voldoen. Het is bovendien verstandig om te controleren of de protocollen die door iPhone OS worden ondersteund zijn ingeschakeld in de implementatie van uw RADIUS-server of server voor identiteitscontrole.
- Neem contact op met de leveranciers van uw hardware en software om te controleren of de nieuwste beveiligingsupdates en firmware zijn geïnstalleerd.
- Als u URL-specifieke proxyinstellingen wilt configureren, plaatst u een PAC-bestand op een webserver die toegankelijk is met de basis-VPN-instellingen en controleert u of op de server het MIME-type 'application/x-ns-proxy-autoconfig' wordt gebruikt. Een andere mogelijkheid is voor uw DNS of DHCP de locatie op te geven van een WPAD-bestand dat op een server is geplaatst die op vergelijkbare wijze toegankelijk is.

IMAP-e-mail

Ook wanneer u geen gebruik maakt van Microsoft Exchange, kunt u een beveiligde, op standaarden gebaseerde e-mailserver implementeren die gebruikmaakt van IMAP en identiteitscontrole via SSL. Met deze techniek kunt u bijvoorbeeld toegang krijgen tot e-mail in Lotus Notes/Domino of Novell GroupWise. De mailservers kunnen zich in een DMZ-subnetwerk of achter een bedrijfsfirewall bevinden, of beide.

iPhone OS biedt ondersteuning voor SSL met 128-bits-codering en X.509-certificaten afkomstig van de belangrijkste certificaatautoriteiten. Het biedt tevens ondersteuning voor sterke identiteitscontrolemethoden, waaronder de veelgebruikte MD5 Challenge-Response- en NTLMv2-methoden.

Richtlijnen voor IMAP-netwerkconfiguratie

- Uit beveiligingsoogpunt is het verstandig om op de server een digitaal certificaat van een vertrouwde certificaatautoriteit (CA) te installeren. De installatie van een certificaat van een CA is een belangrijke stap die ervoor zorgt dat uw proxyserver als een vertrouwde entiteit binnen uw bedrijfsnetwerk wordt beschouwd. Zie “Legitimatie” op pagina 42 voor informatie over de installatie van certificaten op een iPhone.

- Om ervoor te zorgen dat iPhone OS-apparaten e-mail van uw server kunnen ophalen, opent u poort 993 in de firewall en stelt u de proxyserver in op IMAP via SSL.
- Om e-mail te kunnen versturen met de apparaten, moet poort 587, 465 of 25 zijn geopend. Poort 587 wordt als eerste gebruikt en verdient de voorkeur.

LDAP-adreslijsten

Met iPhone OS kunt u toegang krijgen tot op standaarden gebaseerde LDAP-adreslijstservers en globale adreslijsten verstrekken of andere informatie die vergelijkbaar is met de informatie in Microsoft Exchange Global Address List.

Als op het apparaat een LDAP-account is geconfigureerd, wordt ter identificatie van de standaardzoekbasis naar het kenmerk `namingContexts` op het hoofdniveau van de server gezocht. Het zoekbereik is standaard ingesteld op de subhiërarchie.

CalDAV-agenda's

Met de CalDAV-ondersteuning in iPhone OS kunt u globale agenda's en planningen verstrekken voor organisaties die niet werken met Microsoft Exchange. iPhone OS werkt met agendaservers die de CalDAV-standaard ondersteunen.

Agenda's met abonnement

Als u agenda's waarvoor u alleen-lezenbevoegdheden hebt met bedrijfsactiviteiten, zoals feestdagen of planningen voor speciale activiteiten, wilt publiceren, kunt u een abonnement nemen op agenda's en de gegevens naast de Microsoft Exchange- en CalDAV-agenda's weergeven. iPhone OS werkt met agendabestanden in de iCalendar-structuur (.ics).

U kunt agenda's met een abonnement eenvoudig distribueren naar gebruikers door via sms of e-mail de volledige URL te versturen. Wanneer gebruikers op de koppeling tikken, krijgen ze de mogelijkheid om zich te abonneren op de opgegeven agenda.

Bedrijfsprogramma's

Als u bedrijfsprogramma's voor iPhone OS wilt implementeren, installeert u de programma's op de apparaten via iPhone-configuratieprogramma of iTunes. Nadat u een programma op de apparaten van de gebruikers hebt geïnstalleerd, kunt u dit programma het eenvoudigst bijwerken als de gebruikers iTunes op hun Mac of pc hebben geïnstalleerd.

Onlinecertificaatstatusprotocol

Wanneer u digitale certificaten voor iPhone OS-apparaten verstrekt, kunt u overwegen de certificaten met OCSP-ondersteuning uit te geven. Op die manier kan het apparaat bij de OCSP-server nagaan of het certificaat is ingetrokken voordat het certificaat door het apparaat wordt gebruikt.

Kiezen welke beleidsinstellingen voor toegangscodes u voor de apparaten wilt gebruiken

Nadat u hebt opgegeven welke netwerkvoorzieningen en gegevens u aan de gebruikers beschikbaar wilt stellen, moet u bepalen welke beleidsinstellingen voor toegangscodes u wilt implementeren.

Het is verstandig om een toegangscode op de apparaten in te stellen als de netwerken, systemen of programma's van uw bedrijf toegankelijk zijn zonder een wachtwoord of token. Als u gebruikmaakt van identiteitscontrole op basis van certificaten in een 802.1X-netwerk of een Cisco IPSec VPN of als uw inloggegevens door uw bedrijfsprogramma worden bewaard, is het verstandig om het gebruik van een toegangscode met een korte time-outperiode voor de apparaten verplicht te stellen, zodat een apparaat niet kan worden gebruikt als het zoekraakt of gestolen wordt.

De beleidsinstellingen kunnen op de volgende twee manieren op de iPhone, iPod touch en iPad worden ingesteld. Als het apparaat is geconfigureerd voor gebruik van een Microsoft Exchange-account, worden de Exchange ActiveSync-beleidsinstellingen draadloos naar het apparaat verstuurd. Zo kunt u de beleidsinstellingen zonder hulp van de gebruiker toepassen en wijzigen. Zie “Ondersteunde Exchange ActiveSync-beleidsinstellingen” op pagina 9 voor informatie over EAS-beleidsinstellingen.

Als u geen Microsoft Exchange gebruikt, kunt u vergelijkbare beleidsinstellingen toepassen door configuratieprofielen aan te maken. Als u een beleidsinstelling wilt wijzigen, moet u een bijgewerkt profiel naar de gebruikers versturen of het profiel installeren met behulp van iPhone-configuratieprogramma. Zie “Toegangscode” op pagina 35 voor informatie over beleidsinstellingen voor toegangscodes op apparaten.

Als u Microsoft Exchange gebruikt, kunt u uw EAS-beleidsinstellingen ook aanvullen met configuratiebeleidsinstellingen. Op deze manier kunt u toegang geven tot beleidsinstellingen die niet beschikbaar zijn in bijvoorbeeld Microsoft Exchange 2003, of beleidsinstellingen definiëren die specifiek voor iPhone OS-apparaten gelden.

Apparaten configureren

U moet bepalen hoe u elke iPhone, iPod touch of iPad wilt configureren. Deze keuze is deels afhankelijk van het aantal apparaten dat u nu en in de toekomst wilt implementeren en beheren. Als dit aantal klein is, is het voor u en uw gebruikers wellicht het gemakkelijkst om elk apparaat handmatig te configureren. In dat geval moet u de e-mailaccountinstellingen, Wi-Fi-instellingen en VPN-configuratiegegevens direct op het apparaat invoeren. Zie Hoofdstuk 3 voor meer informatie over handmatige configuratie.

Als u van plan bent om een groot aantal apparaten te implementeren, of als u veel verschillende e-mailinstellingen, netwerkinstellingen en certificaten moet installeren, is het verstandig om de apparaten te configureren door de aanmaak en distributie van configuratieprofielen. Met configuratieprofielen kopieert u snel instellingen en toegangscontrolegegevens naar een apparaat. Sommige VPN- en Wi-Fi-instellingen kunnen alleen via een configuratieprofiel worden ingesteld. U moet dan een configuratieprofiel gebruiken om beleidsinstellingen voor toegangscodes in te stellen als u geen Microsoft Exchange gebruikt.

Configuratieprofielen kunnen worden gecodeerd en ondertekend, zodat u het gebruik ervan kunt beperken tot een bepaald apparaat en kunt voorkomen dat gebruikers de instellingen van een profiel kunnen wijzigen. Daarnaast kunt u instellen dat een profiel aan het apparaat is vergrendeld. Op deze manier kan het profiel alleen worden verwijderd door alle gegevens van het apparaat te verwijderen of door een beheerderstoegangscode op te geven.

Of u apparaten nu handmatig configureert of configuratieprofielen gebruikt, u moet hoe dan ook beslissen of u de apparaten zelf configureert of dat u dit door de gebruikers laat doen. Uw beslissing is afhankelijk van de locatie van de gebruikers, of gebruikers binnen uw bedrijf hun eigen IT-apparatuur mogen configureren en de complexiteit van de configuratie die u wilt implementeren. Configuratieprofielen zijn uitermate geschikt voor grote bedrijven, voor externe werknemers en voor gebruikers die niet in staat zijn hun eigen apparaat te configureren.

Als u wilt dat gebruikers zelf hun apparaat kunnen activeren of zelf bedrijfsprogramma's kunnen installeren of bijwerken, moet iTunes op de Mac of pc van de gebruikers zijn geïnstalleerd. Houd er bij de keuze om iTunes al dan niet onder uw gebruikers te verspreiden verder rekening mee dat iTunes ook vereist is voor software-updates van iPhone OS. Zie hoofdstuk 4 voor informatie over de implementatie van iTunes.

Over-the-air-aanmeldingen en -configuratie

'Aanmelding' heeft betrekking op het proces voor de identiteitscontrole van een apparaat en gebruiker, zodat u het proces voor het distribueren van certificaten kunt automatiseren. Digitale certificaten bieden verschillende voordelen voor gebruikers. Zo kunt u deze certificaten gebruiken om de identiteitscontrole uit te voeren voor de toegang tot belangrijke bedrijfsvoorzieningen, zoals Microsoft Exchange ActiveSync, draadloze WPA2-bedrijfsnetwerken en zakelijke VPN-verbindingen. Daarnaast kunt u met identiteitscontrole op basis van certificaten het gebruik van VPN op aanvraag toestaan voor naadloze toegang tot bedrijfsnetwerken.

Naast het gebruik van over-the-air-aanmelding voor de uitgifte van certificaten voor de infrastructuur van de publieke sleutel voor uw bedrijf (Public Key Infrastructure of PKI), kunt u ook apparaatconfiguratieprofielen implementeren. Op deze manier zorgt u ervoor dat alleen vertrouwde gebruikers toegang tot de bedrijfsvoorzieningen kunnen krijgen en dat de apparaten van de gebruikers volgens uw IT-beleidsinstellingen zijn geconfigureerd. Aangezien configuratieprofielen zowel gecodeerd als vergrendeld kunnen zijn, kunnen de instellingen niet worden verwijderd, gewijzigd of met andere personen worden gedeeld. Deze opties zijn beschikbaar in het hieronder beschreven over-the-air-proces en in iPhone-configuratieprogramma wanneer u apparaten configureert terwijl ze zijn aangesloten op uw beheercomputer. Zie hoofdstuk 2 voor meer informatie over het gebruik van iPhone-configuratieprogramma.

Voor de implementatie van over-the-air-aanmelding en -configuratie moet u voorzieningen voor identiteitscontrole, adreslijsten en certificaten ontwikkelen en integreren. U kunt deze voorzieningen implementeren met behulp van standaardwebvoorzieningen. Zodra deze voorzieningen zijn geïmplementeerd, kunnen gebruikers hun apparaten op een veilige manier met identiteitscontrole configureren.

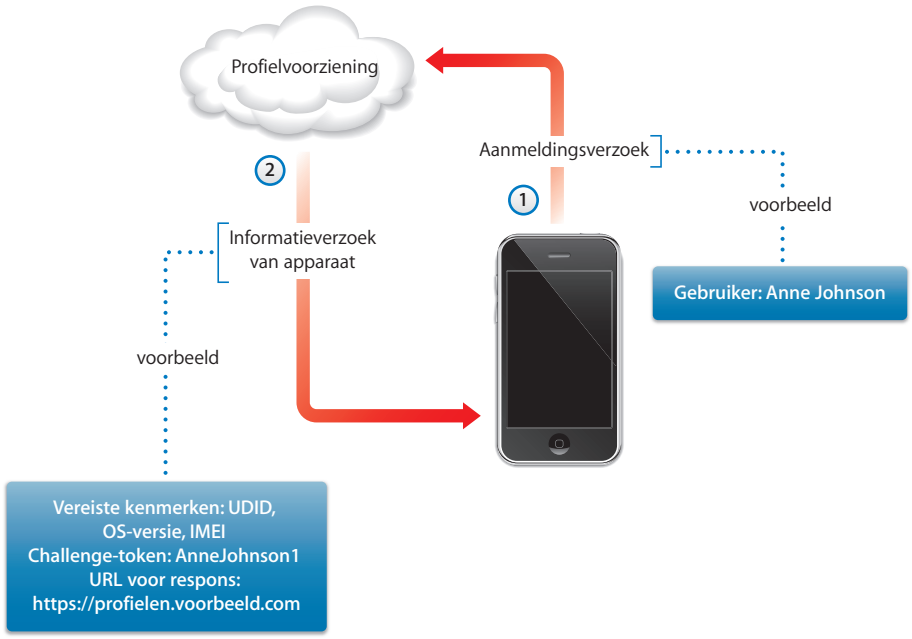
Overzicht van het aanmeldings- en configuratieproces met identiteitscontrole

Om dit proces te kunnen implementeren, moet u een eigen profieldistributievoorziening aanmaken waarmee HTTP-verbindingen worden geaccepteerd, identiteitscontroles voor gebruikers worden uitgevoerd, mobileconfig-profielen worden aangemaakt en het algehele proces wordt beheerd dat in dit gedeelte wordt beschreven.

Daarnaast hebt u een CA (certificaatautoriteit) nodig om de apparaatlegitimaties uit te geven met SCEP (Simple Certificate Enrollment Protocol). Zie “Meer informatie” op pagina 29 voor koppelingen naar PKI, SCEP en verwante onderwerpen.

In het volgende diagram wordt het aanmeldings- en configuratieproces aangegeven dat op de iPhone wordt ondersteund.

Fase 1 - Aanmelding starten

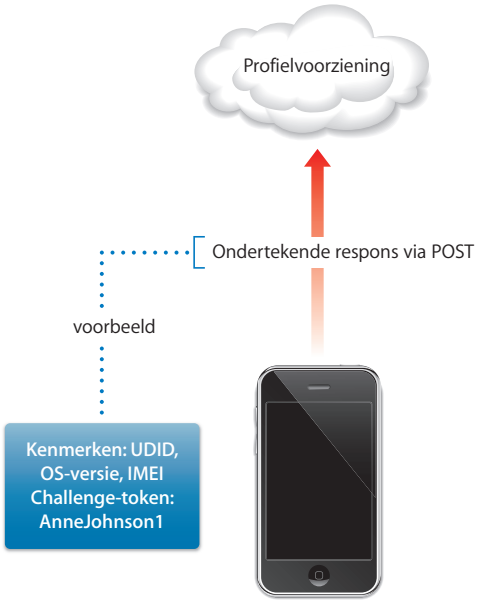


Fase 1 – Aanmelding starten: De aanmelding begint wanneer de gebruiker in Safari de URL opgeeft van de profieldistributievoorziening die u hebt aangemaakt. U kunt deze URL distribueren via sms of e-mail. Met het verzoek tot aanmelding (zie stap 1 in het diagram) moet de identiteit van de gebruiker worden gecontroleerd. Voor de identiteitscontrole kunt u een eenvoudige basiscontrole uitvoeren of u kunt de identiteitscontrole implementeren in uw bestaande adreslijstvoorzieningen.

Als respons stuurt uw voorziening in stap 2 een configuratieprofiel (.mobileconfig). De respons bevat een lijst met kenmerken die het apparaat in de volgende respons moet verstrekken en een vooraf gedeelde sleutel (challenge) waarmee de identiteit van de gebruiker tijdens dit proces kan worden overgebracht, zodat u het configuratieproces voor elke gebruiker kunt aanpassen. De apparaatkenmerken waarom kan worden gevraagd, zijn de iPhone OS-versie, de apparaat-ID (MAC-adres), het producttype (iPhone 3GS retourneert iPhone2,1), de telefoon-ID (IMEI) en de siminformatie (ICCID).

Zie “Fase 1: Serverrespons - voorbeeld” op pagina 95 voor een voorbeeldconfiguratieprofiel voor deze fase.

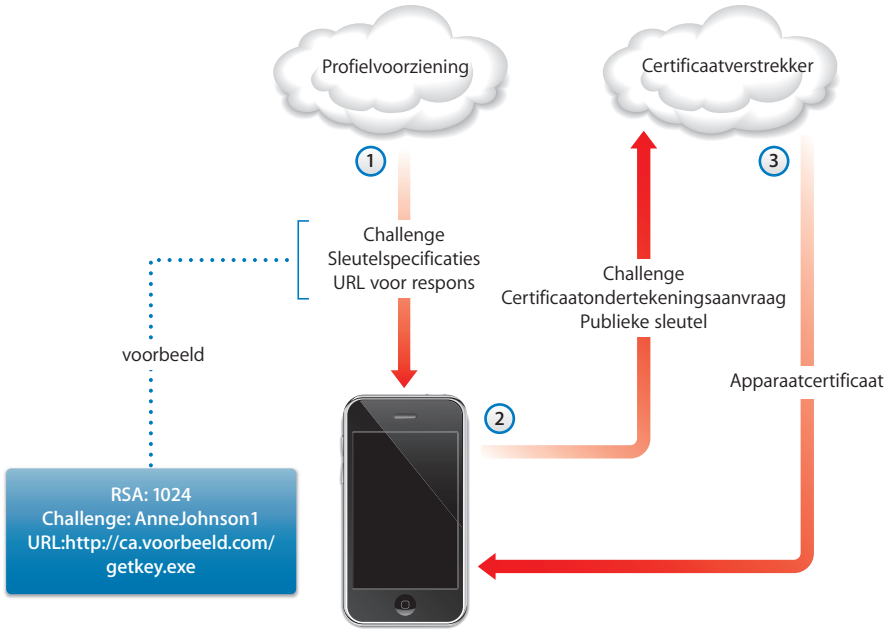
Fase 2 - Identiteitscontrole van apparaat



Fase 2 – Identiteitscontrole van apparaat: Als de gebruiker de installatie van het in fase 1 ontvangen profiel heeft geaccepteerd, worden de gevraagde kenmerken op het apparaat opgezocht, wordt de challengerespons (indien opgegeven) toegevoegd en wordt de respons ondertekend met de eigen identiteit van het apparaat (door Apple uitgegeven certificaat), waarna deze met behulp van 'HTTP Post' wordt teruggestuurd naar de profieldistributievoorziening.

Zie “Fase 2: Apparaatrespons - voorbeeld” op pagina 96 voor een voorbeeldconfiguratieprofiel voor deze fase.

Fase 3 - Installatie van apparaatcertificaat



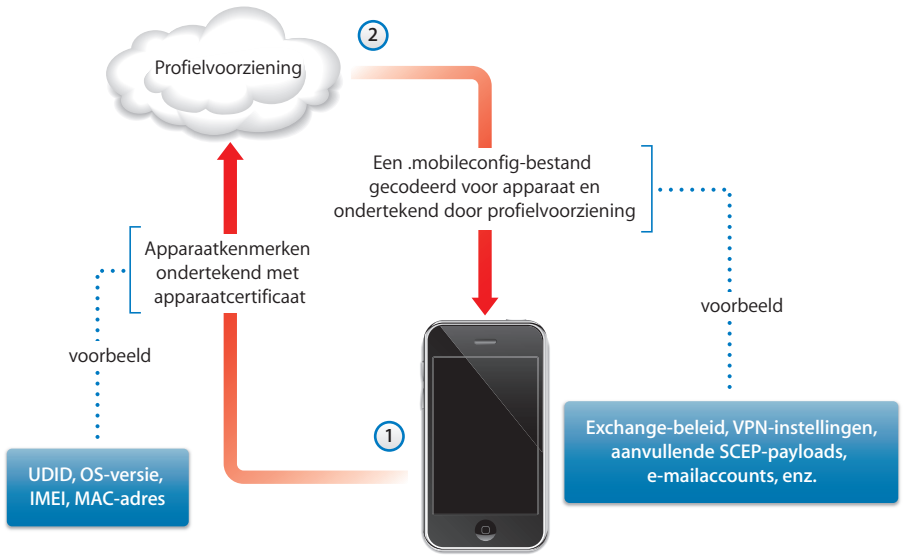
Fase 3 – Installatie van certificaat: In stap 1 verstrekt de profieldistributievoorziening de specificaties die op het apparaat worden gebruikt om een sleutel (RSA 1024) te genereren en om te bepalen naar welke locatie de sleutel moet worden geretourneerd voor certificering met SCEP (Simple Certificate Enrollment Protocol).

In stap 2 moet de SCEP-aanvraag met behulp van de challenge uit het SCEP-pakket in de automatische modus worden verwerkt, zodat de identiteit van de aanvraag kan worden gecontroleerd.

In stap 3 verstrekt de CA een coderingscertificaat voor het apparaat.

Zie “Fase 3: Serverrespons met SCEP-specificaties - voorbeeld” op pagina 96 voor een voorbeeldconfiguratieprofiel voor deze fase.

Fase 4 - Configuratie van apparaat



Fase 4 – Configuratie van apparaat: In stap 1 verstrekt het apparaat de lijst met kenmerken, ondertekend met het coderingscertificaat dat in de vorige door de CA is geleverd.

In stap 2 reageert de profielvoorziening met een gecodeerd .mobileconfig-bestand dat automatisch wordt geïnstalleerd. Het .mobileconfig-bestand moet door de profielvoorziening worden ondertekend. Hiervoor kan bijvoorbeeld het bijbehorende SSL-certificaat worden gebruikt.

Naast de algemene instellingen moeten in dit configuratieprofiel ook de bedrijfsbeleidsinstellingen worden gedefinieerd die u wilt vereisen. U moet het profiel vergrendelen, zodat gebruikers dit niet van het apparaat kunnen verwijderen. Het configuratieprofiel kan aanvullende aanvragen voor de aanmelding van identiteiten met behulp van SCEP bevatten, die worden uitgevoerd wanneer het profiel wordt geïnstalleerd.

Ook kan het apparaat de gebruiker vragen om het profiel bij te werken wanneer een certificaat dat met SCEP is geïnstalleerd, verloopt of ongeldig wordt. Wanneer de gebruiker de aanvraag goedkeurt, wordt het proces herhaald om een nieuw certificaat en profiel te verkrijgen.

Zie “Fase 4: Apparaatrespons - voorbeeld” op pagina 98 voor een voorbeeldconfiguratieprofiel voor deze fase.

Meer informatie

- PKI voor digitale certificaten voor IPSec VPN's op https://cisco.hosted.jivesoftware.com/docs/DOC-3592
- Infrastructuur publieke sleutel op http://nl.wikipedia.org/wiki/Public_key_infrastructure
- IETF SCEP-protocolspecificatie op http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt

Ga voor aanvullende informatie en extra materiaal voor de iPhone, iPod touch en iPad in bedrijfsomgevingen naar www.apple.com/nl/iphone/enterprise/ en www.apple.com/nl/ipad/business/.

Configuratieprofielen aanmaken en implementeren

2

Configuratieprofielen bepalen hoe de iPhone, iPod touch en iPad samenwerken met uw bedrijfssystemen.

Configuratieprofielen zijn XML-bestanden met beveiligings- en beperkingsinstellingen voor het apparaat, VPN-configuratiegegevens, Wi-Fi-instellingen, e-mail- en agenda-accounts en legitimaties voor identiteitscontroles waarmee wordt toegestaan dat de iPhone, iPod touch en iPad in uw bedrijfsomgeving kunnen worden gebruikt.

Met iPhone-configuratieprogramma kunt u configuratieprofielen installeren op apparaten die via USB op een computer zijn aangesloten, of u kunt configuratieprofielen distribueren via e-mail of met behulp van een webpagina. Zodra gebruikers de e-mailbijlage openen of het profiel via Safari downloaden op hun apparaat, wordt aangeboden om het installatieproces te starten.

Als u liever geen configuratieprofielen aanmaakt en distribueert, kunt u de betreffende apparaten ook handmatig configureren. Zie Hoofdstuk 3 voor meer informatie.

iPhone-configuratieprogramma

Met iPhone-configuratieprogramma kunt u configuratieprofielen aanmaken, coderen en installeren, voorzieningenprofielen en bevoegde programma's volgen en installeren, en apparaatgegevens vastleggen, waaronder consolelogbestanden. Het installatieprogramma voor iPhone-configuratieprogramma vindt u in de map /Programma's/Hulpprogramma's/ (Mac) of in Programma's/iPhone Configuration Utility/ (Windows).

Wanneer u iPhone-configuratieprogramma opent, wordt een venster weergegeven dat vergelijkbaar is met het onderstaande venster.

Wat er in het hoofdgedeelte van het venster wordt weergegeven, is afhankelijk van het onderdeel dat u in het linkerpaneel selecteert.

In dit paneel wordt de bibliotheek weergegeven, die de volgende categorieën bevat:

- 'Apparaten' geeft een overzicht van iPhone- en iPod touch-apparaten die op uw computer zijn aangesloten.
- 'Programma's' geeft een overzicht van de programma's die kunnen worden geïnstalleerd op apparaten die op uw computer zijn aangesloten. Om een programma op een apparaat te kunnen uitvoerenen, is mogelijk een voorzieningenprofiel vereist.

- 'Voorzieningenprofielen' geeft een overzicht van alle profielen die toestaan dat het apparaat wordt gebruikt voor het ontwikkelen van programma's voor het iPhone OS, zoals geautoriseerd door Apple Developer Connection. Zie Hoofdstuk 5 voor meer informatie. Daarnaast zorgen voorzieningenprofielen ervoor dat bedrijfsprogramma's die niet via de iTunes Store zijn gedistribueerd, op apparaten kunnen worden uitgevoerd.
- 'Configuratieprofielen' geeft een overzicht van de configuratieprofielen die u eerder hebt aangemaakt. Hier kunt u opgegeven informatie wijzigen en een nieuwe configuratie aanmaken die u naar een gebruiker kunt sturen of op een verbonden apparaat kunt installeren.

In het linkerpaneel staat tevens het onderdeel 'Verbonden apparaten' met een overzicht van de iPhone OS-apparaten die op dat moment op de USB-poort van uw computer zijn aangesloten. Informatie over een verbonden apparaat wordt automatisch opgenomen in de lijst 'Apparaten', zodat deze ook beschikbaar is wanneer het apparaat niet is verbonden. Als een apparaat is verbonden, kunt u ook profielen coderen zodat deze alleen op dat apparaat kunnen worden gebruikt.

Wanneer een apparaat is verbonden, kunt u iPhone-configuratieprogramma gebruiken om configuratieprofielen en programma's op het apparaat te installeren. Zie “Configuratieprofielen installeren met iPhone-configuratieprogramma” op pagina 45,“Programma's installeren met iPhone-configuratieprogramma” op pagina 73 en “Voorzieningenprofielen installeren met iPhone-configuratieprogramma” op pagina 72 voor meer informatie.

Wanneer een apparaat met uw computer is verbonden, kunt u tevens de consolelogbestanden en, indien van toepassing, crashlogbestanden weergeven. Dit zijn dezelfde apparaatlogbestanden die ook in de Xcode-ontwikkelomgeving van Mac OS X beschikbaar zijn.

Configuratieprofielen aanmaken

In dit document komen de termen 'configuratieprofiel' en 'payload' (lading) voor. Een configuratieprofiel is het volledige bestand waarmee een of meer instellingen op een iPhone, iPod touch of iPad worden geconfigureerd. Een payload is een afzonderlijke verzameling van een bepaald type instellingen binnen het configuratieprofiel, bijvoorbeeld de VPN-instellingen.

U kunt ervoor kiezen om slechts één configuratieprofiel aan te maken dat alle benodigde payloads, maar het is het overwegen waard om voor certificaten en instellingen afzonderlijke profielen aan te maken. In dat geval kunt u namelijk de gegevens per type bijwerken en distribueren. Bovendien blijven reeds geïnstalleerde certificaten dan behouden wanneer gebruikers een nieuw profiel met bijvoorbeeld gewijzigde VPN- of accountinstellingen installeren.

Voor veel payloads kunt u gebruikersnamen en wachtwoorden opgeven. Als u deze informatie weglaat, kan het profiel door meerdere gebruikers worden gebruikt. De gebruiker moet in dit geval de ontbrekende informatie opgeven tijdens de installatie van het profiel. Als u het profiel voor elke gebruiker personaliseert en wachtwoorden gebruikt, moet u het profiel gecodeerd distribueren om de inhoud ervan te beveiligen. Zie “Configuratieprofielen installeren” op pagina 44 voor meer informatie.

Als u een nieuw configuratieprofiel wilt aanmaken, klikt u op de knop 'Nieuw' in de knoppenbalk van iPhone-configuratieprogramma. Via de lijst met payloads kunt u payloads aan het profiel toevoegen. Vervolgens kunt u de payloads wijzigen door opties in het wijzigingspaneel in te voeren en te selecteren. Verplichte velden zijn gemarkeerd met een rode pijl. Voor sommige instellingen, zoals 'Wi-Fi', kunt u configuraties toevoegen door op de knop met het plusteken te klikken. Om een configuratie te verwijderen, klikt u in het wijzigingspaneel op de knop met het minteken.

Om een payload te wijzigen, selecteert u het gewenste onderdeel in de lijst met payloads, klikt u op de knop 'Configureer' (Mac) of 'Configureren' (Windows) en voert u de gegevens in, zoals hieronder wordt beschreven.

Geautomatiseerde aanmaak van configuratieprofielen

Het is ook mogelijk om de aanmaak van configuratiebestanden te automatiseren met AppleScript (op een Mac) of C# Script (onder Windows). Als u de ondersteunde methoden en de bijbehorende syntaxis wilt bekijken, doet u het volgende:

- *Mac OS X:* Gebruik Scripteditor om het AppleScript-woordenboek voor iPhone-configuratieprogramma te openen.
- *Windows*: Gebruik Visual Studio om de methodeaanroepen van iPCUScripting.dll weer te geven.

Op een Mac voert u een script uit met het AppleScript-commando 'Tell'. Onder Windows geeft u de scriptnaam als commandoregelparameter door aan iPhone-configuratieprogramma.

Zie Bijlage C, “Voorbeeldscripts” voor een aantal voorbeelden.

Algemeen

Hier geeft u de naam en aanduiding van het profiel op en geeft u aan of gebruikers het profiel na installatie kunnen verwijderen.

De naam die u hier opgeeft, verschijnt in de lijst met profielen en wordt weergegeven op het apparaat als het configuratieprofiel is geïnstalleerd. De opgegeven naam hoeft niet uniek te zijn. Wel is van belang dat u een beschrijvende naam gebruikt waaraan het profiel eenvoudig te herkennen is.

De aanduiding van de configuratie moet wel uniek zijn en moet aan deze notatie voldoen: com.bedrijfsnaam.profielaanduiding, waarbij profielaanduiding een omschrijving van het profiel is. (Bijvoorbeeld com.mijnbedrijf.kantooraanhuis.)

De aanduiding is belangrijk omdat tijdens de installatie van het profiel de waarde wordt vergeleken met de aanduiding van de profielen die al op het apparaat zijn geïnstalleerd. Als de aanduiding uniek is, wordt de informatie van het profiel overgezet naar het apparaat. Als de aanduiding gelijk is aan die van een reeds geïnstalleerd profiel, dan worden de huidige instellingen van het apparaat overschreven door de nieuwe informatie in het profiel, met uitzonderingen van Exchange-instellingen. Om een Exchange-account te wijzigen, moet u het profiel eerst handmatig verwijderen zodat de aan de account gekoppelde gegevens kunnen worden opgeschoond.

Om te voorkomen dat een gebruiker een op een apparaat geïnstalleerd profiel verwijdert, kiest u een optie uit het venstermenu 'Beveiliging'. Als u de optie 'Met identiteitscontrole' kiest, kunt u het wachtwoord voor autorisatie opgeven dat moet worden ingevoerd om het profiel van het apparaat te kunnen verwijderen. Als u de optie 'Nooit' selecteert, kan het profiel worden bijgewerkt met een nieuwe versie, maar kan het profiel niet worden verwijderd.

Toegangscode

Als u geen gebruikmaakt van een Exchange-toegangscodebeleid, kunt u deze payload gebruiken om het gewenste toegangscodebeleid voor het apparaat in te stellen. U kunt bijvoorbeeld opgeven of een toegangscode vereist is om het apparaat te kunnen gebruiken, aan welke voorwaarden de toegangscode moet voldoen en hoe vaak die moet worden vernieuwd. Wanneer het configuratieprofiel wordt geladen, moet de gebruiker een toegangscode opgeven die voldoet aan de voorwaarden die u hier selecteert, anders wordt het profiel niet geïnstalleerd.

Als u gebruikmaakt van een toegangscodebeleid voor het apparaat en een Exchange-toegangscodebeleid, worden beide samengevoegd en wordt het strengste beleid uitgevoerd. Zie “Microsoft Exchange ActiveSync” op pagina 8 voor informatie over ondersteunde beleidsinstellingen van Exchange ActiveSync.

De volgende opties zijn beschikbaar:

- 'Toegangscode op apparaat vereist':Verplicht het gebruik van een toegangscode voordat het apparaat kan worden gebruikt. Als geen code is vereist, kan iedereen gebruikmaken van alle functionaliteit en gegevens op dit apparaat.
- 'Sta eenvoudige waarde toe' (Mac) of 'Eenvoudige waarde toestaan' (Windows):Staat toe dat gebruikers een toegangscode kiezen waarin gebruik wordt gemaakt van een opeenvolgende reeks tekens of waarin tekens worden herhaald. Een eenvoudige toegangscode is bijvoorbeeld '3333' of 'DEFG'.
- 'Alfanumerieke waarde vereist':Toegangscodes moeten minimaal één letter bevatten.
- 'Minimale lengte toegangscode':Het kleinste aantal tekens waaruit de toegangscode mag bestaan.
- 'Minimale aantal complexe tekens': Het kleinste aantal niet-alfanumerieke tekens (zoals $, & en !) waaruit de toegangscode moet bestaan.
- 'Maximale gebruiksduur toegangscode' (in dagen): Het aantal dagen waarna gebruikers hun toegangscode moeten wijzigen.
- 'Automatisch slot' (in minuten): Als het apparaat gedurende de opgegeven periode niet wordt gebruikt, wordt het automatisch vergrendeld. Het apparaat kan worden ontgrendeld door de toegangscode op te geven.
- 'Geschiedenis toegangscodes': Nieuwe toegangscodes worden niet geaccepteerd als deze gelijk zijn aan eerder gebruikte toegangscodes. U kunt opgeven hoeveel eerdere toegangscodes voor deze vergelijking bewaard moeten blijven.
- 'Geldigheid toegangscode bij vergrendeling': Hiermee wordt aangegeven hoe snel het apparaat na gebruik weer kan worden ontgrendeld, zonder dat hierbij om de toegangscode wordt gevraagd.

- 'Maximale aantal mislukte pogingen': Hiermee wordt bepaald hoeveel pogingen mogen worden gedaan om de juiste toegangscode in te voeren voordat het apparaat wordt gewist. Als u deze instelling niet wijzigt, treedt na zes mislukte pogingen een vertraging op, zodat het even duurt voordat de toegangscode opnieuw kan worden ingevoerd. De vertraging wordt na iedere mislukte poging langer. Na de elfde mislukte poging worden alle gegevens en instellingen veilig van het apparaat gewist. De vertraging wordt altijd na de zesde poging gestart, dus als u hier een waarde van 6 of lager opgeeft, vindt geen vertraging plaats en wordt het apparaat direct gewist zodra de opgegeven waarde wordt overschreden.

Beperkingen

Met deze payload kunt u opgeven tot welke apparaatvoorzieningen de gebruiker toegang heeft.

- 'Sta expliciet materiaal toe' (Mac) of 'Expliciet materiaal toestaan' (Windows):Als deze optie is uitgeschakeld, wordt expliciet muziek- of videomateriaal dat via de iTunes Store is aangeschaft,verborgen. Expliciet materiaal wordt als zodanig aangeduid door de aanbieders van het materiaal (zoals platenlabels) bij de verkoop via de iTunes Store.
- 'Sta gebruik van Safari toe' (Mac) of 'Gebruik van Safari toestaan' (Windows): Als deze optie is uitgeschakeld, wordt het programma Safari uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Met deze optie kunt u ook voorkomen dat gebruikers webknipsels kunnen openen.
- 'Sta gebruik van YouTube toe' (Mac) of 'Gebruik van YouTube toestaan' (Windows): Als deze optie is uitgeschakeld, wordt het programma YouTube uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd.
- 'Sta gebruik van iTunes Music Store toe' (Mac) of 'Gebruik van iTunes Music Store toestaan' (Windows): Als deze optie is uitgeschakeld, wordt de iTunes Music Store uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Gebruikers kunnen materiaal niet vooraf bekijken of beluisteren en geen materiaal aanschaffen of downloaden.
- 'Sta installatie van programma's toe' (Mac) of 'Installatie van programma's toestaan' (Windows): Als deze optie is uitgeschakeld, wordt de App Store uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Gebruikers kunnen geen programma's installeren of bijwerken.
- 'Sta gebruik van camera toe' (Mac) of 'Gebruik van camera toestaan' (Windows): Als deze optie is uitgeschakeld, wordt de camera volledig uitgeschakeld en wordt het camerasymbool uit het beginscherm verwijderd. Gebruikers kunnen geen foto's maken.
- 'Sta schermafbeelding toe' (Mac) of 'Schermafbeelding toestaan' (Windows): Als deze optie is uitgeschakeld, kunnen gebruikers geen schermafbeelding bewaren.

Wi-Fi

Met deze payload geeft u de instellingen voor verbinding met uw draadloze netwerk op. U kunt meerdere netwerkconfiguraties opgeven door op de knop met het plusteken te klikken.

De onderstaande instellingen zijn verplicht. Alleen indien deze overeenkomen met de instellingen van uw netwerk, kan de gebruiker een verbinding tot stand brengen.

- 'SSID (Service Set Identifier'):Hier geeft u de SSID op van het draadloze netwerk waarmee verbinding wordt gemaakt.
- 'Verborgen netwerk': Hiermee geeft u op of het netwerk zijn identiteit kenbaar maakt.
- 'Beveiligingstype': Hier selecteert u een methode voor identiteitscontrole voor het netwerk. De volgende opties zijn beschikbaar voor zowel persoonlijke netwerken als bedrijfsnetwerken.
  - 'Geen': Het netwerk maakt geen gebruik van identiteitscontrole.
  - 'WEP': Het netwerk maakt alleen gebruik van WEP-identiteitscontrole.
  - 'WPA/WPA 2': Het netwerk maakt alleen gebruik van WPA-identiteitscontrole.
  - 'Willekeurig': Het apparaat maakt gebruik van WEP- of WPA-identiteitscontrole bij de totstandbrenging van de netwerkverbinding, maar kan geen verbinding maken met netwerken die geen gebruik maken van identiteitscontrole.
- 'Wachtwoord': Hier geeft u het wachtwoord op van het draadloze netwerk waarmee verbinding wordt gemaakt. Als u geen wachtwoord opgeeft, wordt de gebruiker gevraagd een wachtwoord in te voeren.

Instellingen op bedrijfsniveau

In dit gedeelte geeft u instellingen op voor verbinding met bedrijfsnetwerken. Deze instellingen verschijnen alleen als u uit het venstermenu 'Beveiligingstype' een optie op bedrijfsniveau hebt gekozen.

In het paneel 'Protocollen' geeft u op welke EAP-typen worden gebruikt voor de identiteitscontrole en stelt u de gewenste EAP-FAST Protected Access Credential-configuratie in.

In het paneel 'Identiteitscontrole' geeft u de inloggegevens op, zoals de gebruikersnaam en het protocol voor de identiteitscontrole. Als u via de payload 'Legitimatie' een identiteit hebt geïnstalleerd, kunt u dit kiezen uit het venstermenu 'Identiteitscertificaat'.

In het paneel 'Vertrouwen' geeft u op welke certificaten kunnen worden vertrouwd voor controle van de server voor identiteitscontrole die voor de Wi-Fi-verbinding is ingesteld. De lijst met vertrouwde certificaten bevat de certificaten die via de payload 'Legitimatie' zijn toegevoegd. Hier selecteert u welke certificaten kunnen worden vertrouwd. Onder 'Vertrouwde certificaatnamen van server' voegt u de servers voor identiteitscontrole toe die kunnen worden vertrouwd. U kunt hier een specifieke server opgeven, bijvoorbeeld 'server.mijnbedrijf.com', of een gedeeltelijke naam, bijvoorbeeld '*.mijnbedrijf.com'.

Door 'Sta vertrouwensuitzonderingen toe' (Mac) of 'Vertrouwensuitzonderingen toestaan' (Windows) in te schakelen, laat u de keuze aan de gebruiker om een server al dan niet te vertrouwen ingeval er geen vertrouwensketen kan worden vastgesteld. Als u wilt voorkomen dat er een dialoogvenster verschijnt en u alleen verbindingen met een vertrouwde voorziening wilt toestaan, schakelt u dit aankruisvak uit en neemt u alle benodigde certificaten op in een profiel.

VPN

Met deze payload kunt u de VPN-instellingen voor verbinding met uw netwerk opgeven. U kunt meerdere VPN-verbindingen opgeven door op de knop met het plusteken te klikken.

Zie “VPN” op pagina 11 voor informatie over ondersteunde VPN-protocollen en -methoden voor identiteitscontrole. Welke opties beschikbaar zijn, is afhankelijk van het geselecteerde protocol en de geselecteerde methode voor identiteitscontrole.

VPN op aanvraag

Voor IPSec-configuraties op basis van certificaten kunt u VPN op aanvraag inschakelen, zodat automatisch een VPN-verbinding tot stand wordt gebracht wanneer u toegang een bepaald domein probeert te krijgen.

De volgende opties voor VPN op aanvraag zijn beschikbaar:

Instelling	Beschrijving
'Maak altijd verbinding'	Er wordt een VPN-verbinding geïnitieerd voor elk adres dat overeenkomt met het opgegeven domein.
'Maak nooit verbinding'	Er wordt geen VPN-verbinding geïnitieerd voor adressen die overeenkomen met het opgegeven domein, maar als de VPN-verbinding al actief is, kan deze worden gebruikt.
'Maak verbinding indien nodig'	Hiermee wordt alleen een VPN-verbinding geïnitieerd voor adressen die overeenkomen met het opgegeven domein als het opzoeken van het adres in DNS is mislukt.

De actie geldt voor alle overeenkomende adressen. Adressen worden vergeleken op basis van een eenvoudige tekenreeksvergelijking die achteraan begint. Het adres ".voorbeeld.org" komt overeen met "support.voorbeeld.org" en "sales.voorbeeld.org", maar niet met "www.prive-voorbeeld.org". Als u het domein echter opgeeft als "voorbeeld.org" (dus zonder punt aan het begin), komt het wel overeen met "www.prive-voorbeeld.org" en alle andere voorbeeldadressen.

Houd er rekening mee dat LDAP-verbindingen geen VPN-verbinding initiëren. Als de VPN-verbinding nog niet door een ander programma (zoals Safari) tot stand is gebracht, zal het opzoeken van het adres in LDAP mislukken.

VPN-proxy

iPhone ondersteunt handmatige VPN-proxy en automatische proxyconfiguratie met PAC of WPAD. Om een VPN-proxy op te geven, selecteert u een optie uit het venstermenu 'Proxyconfiguratie'.

Voor automatische proxyconfiguraties op basis van PAC selecteert u 'Automatisch' uit het venstermenu en geeft u vervolgens de URL van een PAC-bestand op. Zie “Meer informatie” op pagina 61 voor informatie over de PACS-opties en de -bestandsstructuur.

Voor WPAD-configuraties (Web Proxy Autodiscovery) selecteert u 'Automatisch' uit het venstermenu. Laat het veld 'URL proxysever' leeg. Het WPAD-bestand wordt op de iPhone aangevraagd met behulp van DHCP en DNS. Zie “Meer informatie” op pagina 61 voor informatie over WPAD.

E-mail

Met deze payload kunt u de POP- of IMAP-e-mailaccounts voor de gebruiker opgeven. Als u een Exchange-account toevoegt, raadpleegt u de onderstaande Exchange-instellingen.

Bepaalde e-mailinstellingen die u in een profiel opneemt, zoals de accountnaam, het wachtwoord en alternatieve SMTP-servers, kunnen door de gebruikers worden aangepast. Als u een of meer van deze gegevens uit het profiel weglaat, moeten de gebruikers deze opgeven wanneer ze van hun account gebruik willen maken.

U kunt meerdere e-mailaccounts opgeven door op de knop met het plusteken (+) te klikken.

Exchange

Met deze payload kunt u de instellingen voor uw Exchange-server opgeven. U kunt een profiel voor een bepaalde gebruiker aanmaken en alvast de gebruikersnaam, de hostnaam en het e-mailadres opgeven, maar het is ook mogelijk om alleen de hostnaam op te geven. In dat geval wordt de gebruiker bij de installatie van het profiel gevraagd om de overige gegevens op te geven.

Wanneer u een gebruikersnaam, hostnaam en SSL-instelling opgeeft in het profiel, kan de gebruiker deze gegevens niet wijzigen op het apparaat.

Per apparaat kunt u slechts één Exchange-account instellen. Voor andere e-mailaccounts, inclusief eventuele Exchange-IMAP-accounts, heeft de toevoeging van een Exchange-account geen gevolgen. Exchange-accounts die met behulp van een profiel worden toegevoegd, kunnen alleen worden verwijderd door het profiel te verwijderen.

Standaard wordt de synchronisatie van contact-, agenda- en e-mailgegevens door Exchange verzorgd. De gebruiker kan deze instellingen aanpassen op het apparaat door 'Instellingen' > 'Accounts' te kiezen. Een van de instellingen die kan worden gewijzigd, is het aantal dagen waarvan de gegevens moeten worden gesynchroniseerd.

Als u het aankruisvak 'Gebruik SSL' (Mac) of 'SSL gebruiken' (Windows) inschakelt, moet u in de payload 'Legitimatie' de certificaten opgeven die nodig zijn om de identiteitscontrole voor de verbinding uit te voeren.

Om een certificaat te verstrekken waarmee de gebruiker bij de Exchange ActiveSync-server wordt geïdentificeerd, klikt u op de knop met het plusteken en selecteert u vervolgens een identiteitscertificaat uit Sleutelhangertoegang (Mac) of Certificaatarchief (Windows). Nadat u een certificaat hebt toegevoegd, kunt u de naam voor de legitimatie voor de identiteitscontrole opgeven, indien dat voor de ActiveSync-configuratie nodig is. U kunt ook de wachtzin van het certificaat insluiten in het configuratieprofiel. Als u geen wachtzin opgeeft, wordt de gebruiker bij de installatie van het profiel gevraagd de wachtzin in te voeren.

LDAP-instellingen

Met deze payload kunt u de instellingen voor verbinding met een LDAPv3-adreslijst opgeven. Voor elke adreslijst kunt u meerder zoekbasissen opgeven. Om meerdere adreslijstverbindingen te configureren, klikt u op de knop met het plusteken.

Als u het aankruisvak 'Gebruik SSL' (Mac) of 'SSL gebruiken' (Windows) inschakelt, moet u in de payload 'Legitimatie' de certificaten opgeven die nodig zijn om de identiteitscontrole voor de verbinding uit te voeren.

CalDAV

Met deze payload kunt u accountinstellingen opgeven voor verbinding met een agendaserver die CalDAV ondersteunt. Deze accounts worden toegevoegd aan het apparaat. Wanneer het profiel wordt geïnstalleerd, moeten gebruikers, net als bij Exchange-accounts, handmatig de gegevens invoeren die u uit het profiel hebt weggelaten, zoals hun wachtwoord.

Als u het aankruisvak 'Gebruik SSL' (Mac) of 'SSL gebruiken' (Windows) inschakelt, moet u in de payload 'Legitimatie' de certificaten opgeven die nodig zijn om de identiteitscontrole voor de verbinding uit te voeren.

U kunt meerdere accounts configureren door op de knop met het plusteken te klikken.

Agenda's met abonnement

Met deze payload kunt u agenda's waarvoor u alleen-lezenbevoegdheden hebt toevoegen aan het programma Agenda op het apparaat. U kunt meerdere abonnementen configureren door op de knop met het plusteken te klikken.

Ga naar www.apple.com/nl/downloads/macosx/calendars/ voor een overzicht van de publieke agenda's waarop u zich kunt abonneren.

Als u het aankruisvak 'Gebruik SSL' (Mac) of 'SSL gebruiken' (Windows) inschakelt, moet u in de payload 'Legitimatie' de certificaten opgeven die nodig zijn om de identiteitscontrole voor de verbinding uit te voeren.

Webknipsel

Met deze payload kunt u webknipsels toevoegen aan het beginscherm van het apparaat van de gebruiker. Met webknipsels kunnen gebruikers snel toegang krijgen tot favoriete webpagina's.

Controleer of de URL die u invoert, het voorvoegsel http:// of https:// bevat. Als dit niet het geval is, functioneert het webknipsel niet naar behoren. Als u bijvoorbeeld de onlineversie van de *iPhone-gebruikershandleiding* wilt toevoegen aan het beginscherm, geeft u de volgende URL van het webknipsel op: http://help.apple.com/iphone/

Om een aangepast symbool toe te voegen, selecteert u een grafisch bestand met de structuur 'gif', 'jpeg' of 'png' en met een afmeting van 59 x 60 pixels. De afbeelding wordt automatisch geschaald en bijgesneden, en indien nodig geconverteerd naar de structuur 'png'.

Legitimatie

Met deze payload kunt u de certificaten en identiteiten voor het apparaat opgeven. Zie “Certificaten en identiteiten” op pagina 12 voor informatie over ondersteunde structuren.

Installeer tegelijk met de legitimaties ook de tijdelijke certificaten die nodig zijn om een keten tot stand te brengen met een vertrouwd certificaat op het apparaat. Zie voor een lijst met vooraf geïnstalleerde roots het Apple Support-artikel op http://support.apple.com/kb/HT2185?viewlocale=nl_NL.

Als u een identiteit toevoegt voor gebruik met Microsoft Exchange, gebruikt u de payload 'Exchange'. Zie “Exchange” op pagina 40.

Legitimaties toevoegen in Mac OS X

1. Klik op de knop met het plusteken.
2. Er verschijnt een venster waarin een bestand kan worden geselecteerd. Selecteer het bestand 'PKCS1' of 'PKSC12' en klik vervolgens op 'Open'.

   Als het te installeren certificaat of de te installeren identiteit zich in uw sleutelhanger bevindt, gebruikt u Sleutelhangertoegang om het certificaat of de identiteit in de .p12-structuur te exporteren. Sleutelhangertoegang bevindt zich in de map /Programma's/Hulpprogramma's. Raadpleeg Sleutelhangertoegang Help (beschikbaar in het Help-menu wanneer Sleutelhangertoegang actief is) voor meer informatie.

Om meer legitimaties aan het configuratieprofiel toe te voegen, klikt u nogmaals op de knop met het plusteken.

Legitimaties toevoegen in Windows

1. Klik op de knop met het plusteken.
2. Selecteer de legitimatie die u wilt installeren in Certificaatarchief van Windows.

   Als de legitimatie niet beschikbaar is in uw persoonlijke certificaatarchief, moet u deze toevoegen en moet u de persoonlijke sleutel markeren als exporteerbaar. Dit kunt u doen met behulp van de wizard Certificaat importeren. Voor het toevoegen van basiscertificaten is beheerderstoegang tot de computer vereist. Daarnaast moeten basiscertificaten aan het persoonlijke archief worden toegevoegd.

Als u meerdere configuratieprofielen gebruikt, moet u ervoor zorgen dat er geen dubbele certificaten aanwezig zijn. Het is niet mogelijk meerdere exemplaren van hetzelfde certificaat te installeren.

In plaats van certificaten te installeren via een configuratieprofiel, kunt u gebruikers de certificaten ook naar hun apparaat laten downloaden via een webpagina in Safari. Bovendien is het mogelijk om de certificaten per e-mail naar de gebruikers te sturen. Zie “Identiteiten en rootcertificaten installeren” op pagina 60 voor meer informatie. U kunt ook gebruikmaken van de SCEP-instellingen (zie hieronder) om aan te geven hoe certificaten over-the-air op het apparaat worden ontvangen wanneer het profiel is geïnstalleerd.

SCEP

Met de SCEP-payload kunt u instellingen opgeven waarmee het apparaat met behulp van SCEP (Simple Certificate Enrollment Protocol) certificaten van een CA kan ontvangen.

Instelling	Beschrijving
URL	Het adres van de SCEP-server.
Naam	Een willekeurige tekenreeks die door de certificaatautoriteit kan worden begrepen. U kunt de naam bijvoorbeeld gebruiken om een onderscheid te maken tussen de verschillende exemplaren.
Onderwerp	De weergave van een X.500-naam, aangeduid als een array bestaande uit een object-ID en een waarde. Bijvoorbeeld: '/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar', wat het volgende inhoudt: [[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]]
Challenge	Een vooraf gedeeld geheim dat de SCEP-server kan gebruiken om de aanvraag of gebruiker te identificeren.
Sleutelgrootte en -gebruik	Selecteer een sleutelgrootte en geef met behulp van de aankruisvakken onder dit veld aan hoe de sleutel kan worden gebruikt.
Vingerafdruk	Als de certificaatautoriteit gebruikmaakt van HTTP, gebruikt u dit veld om de vingerafdruk van het CA-certificaat op te geven op basis waarvan het apparaat de echtheid van de respons van de CA tijdens het aanmeldingsproces kan bevestigen. U kunt een SHA1- of MD5-vingerafdruk invoeren of een certificaat selecteren om daarvan de handtekening te importeren.

Zie “Over-the-air-aanmeldingen en -configuratie” op pagina 24 voor meer informatie over de manier waarop certificaten draadloos op de iPhone kunnen worden ontvangen.

Geavanceerd

Met deze payload kunt u de toegangspuntinstellingen (APN-instellingen) en de proxyinstellingen van het mobieletelefoonnetwerk van het apparaat wijzigen. Deze instellingen bepalen hoe het apparaat verbinding maakt met het netwerk van de telecomaanbieder. U dient deze instellingen alleen te wijzigen op aanwijzing van een netwerkdeskundige van de telecomaanbieder. Als de instellingen in dit paneel onjuist zijn, kan het apparaat geen gegevens ophalen via het mobieletelefoonnetwerk. Onjuiste wijzigingen in deze instellingen kunt u ongedaan maken door het profiel van het apparaat te verwijderen. U wordt aangeraden APN-instellingen te definiëren in een configuratieprofiel dat losstaat van andere bedrijfsinstellingen, omdat profielen waarin APN-gegevens zijn opgegeven, moeten worden ondertekend door de aanbieder van de mobieletelefoniedienst.

iPhone OS ondersteunt APN-gebruikersnamen van maximaal 20 tekens en wachtwoorden van maximaal 32 tekens.

Configuratieprofielen wijzigen

Om een configuratieprofiel te wijzigen, selecteert u in iPhone-configuratieprogramma het gewenste profiel in de lijst met configuratieprofielen en wijzigt u de instellingen in de lijst met payloads en de wijzigingspanelen. U kunt een profiel ook importeren door 'Archief' > 'Voeg toe aan bibliotheek' (Mac) of 'Bestand' > 'Aan bibliotheek toevoegen' (Windows) te kiezen en vervolgens het juiste .mobileconfig-bestand te selecteren. Als de instellingenpanelen niet worden weergegeven, kiest u 'Weergave'> 'Toon details' (Mac) of 'Beeld' > 'Details tonen' (Windows).

Op basis van de waarde in het veld 'Aanduiding' in de payload 'Algemeen' wordt op het apparaat bepaald of het om een nieuw profiel of een bijgewerkte versie van een bestaand profiel gaat. Als u wilt dat het bijgewerkte profiel het reeds geïnstalleerde profiel overschrijft, laat u de aanduiding ongemoeid.

Voorzieningenprofielen en programma's installeren

U kunt met iPhone-configuratieprogramma programma's en voorzieningenprofielen voor distributie installeren op apparaten die op de computer zijn aangesloten. Zie Hoofdstuk 5, “Programma's implementeren”, op pagina 70 voor meer informatie.

Configuratieprofielen installeren

Als u een profiel hebt aangemaakt, kunt u een apparaat verbinden en het profiel installeren met iPhone-configuratieprogramma.

U kunt het profiel ook per e-mail of via een website naar gebruikers distribueren. Zodra gebruikers de e-mailbijlage openen of het profiel downloaden op hun apparaat, wordt aangeboden om het installatieproces te starten.

Configuratieprofielen installeren met iPhone-configuratieprogramma

U kunt configuratieprofielen rechtstreeks installeren op apparaten die zijn bijgewerkt met iPhone OS 3.0 of hoger en die op uw computer zijn aangesloten. Bovendien kunt u met iPhone-configuratieprogramma eerder geïnstalleerde profielen verwijderen.

Een configuratieprofiel installeren

1. Sluit het apparaat met behulp van een USB-kabel op uw computer aan.

   Na enkele ogenblikken verschijnt het apparaat in de lijst 'Apparaten' in iPhone-configuratieprogramma.
2. Selecteer het apparaat en klik vervolgens op de tab 'Configuratieprofielen'.
3. Selecteer een configuratieprofiel in de lijst en klik op 'Installeer' (Mac) of 'Installeren' (Windows).
4. Tik op het apparaat op 'Installeer' om het profiel te installeren.

   Wanneer u het profiel via USB rechtstreeks op een apparaat installeert, wordt het configuratieprofiel automatisch ondertekend en gecodeerd voordat het naar het apparaat wordt gekopieerd.

Configuratieprofielen per e-mail distribueren

U kunt configuratieprofielen per e-mail distribueren. Gebruikers kunnen het profiel installeren door het bericht op hun apparaat te ontvangen en vervolgens op de bijlage te tikken.

Een profiel per e-mail distribueren

1. Klik op de knop 'Deel' (Mac) of 'Delen' (Windows) in de knoppenbalk van iPhone-configuratieprogramma.

   Selecteer een beveiligingsoptie in het venster dat wordt weergegeven:

   a. 'Geen':Het bestand .mobileconfig wordt in platte tekst aangemaakt. Dit bestand kan op elk gewenst apparaat worden geïnstalleerd. Bepaalde gegevens in het bestand zijn onleesbaar gemaakt om ongewenst meekijken te voorkomen als het bestand wordt bekeken.

   b. 'Onderteken configuratieprofiel' (Mac) of 'Configuratieprofiel ondertekenen' (Windows): Het bestand .mobileconfig wordt ondertekend en wordt niet op een apparaat geïnstalleerd als het bestand is gewijzigd. Bepaalde velden zijn onleesbaar gemaakt om ongewenst meekijken te voorkomen als het bestand wordt bekeken. Na de installatie kan het profiel alleen worden bijgewerkt door een profiel met dezelfde aanduiding die is ondertekend met hetzelfde exemplaar van iPhone-configuratieprogramma.

c 'Onderteken en codeer profiel' (Mac) of 'Profiel ondertekenen en coderen' (Windows): Het profiel wordt ondertekend zodat dit niet kan worden gewijzigd. Bovendien wordt de volledige inhoud van het profiel gecodeerd zodat het profiel niet kan worden bekeken en alleen op een specifiek apparaat kan worden geïnstalleerd. Deze optie is aanbevolen voor profielen met wachtwoorden. Voor elk apparaat dat u in de lijst 'Apparaten' selecteert, wordt een afzonderlijk .mobileconfig-bestand aangemaakt. Als een apparaat niet in de lijst wordt weergegeven, is het apparaat niet eerder op de computer aangesloten zodat de coderingssleutel niet kan worden opgehaald, of is het apparaat niet bijgewerkt naar iPhone OS 3.0 of hoger.

2 Klik op 'Deel' (Mac) of 'Delen' (Windows). Er wordt een nieuw bericht in Mail (Mac OS X) of Outlook (Windows) geopend, met de profielen als ongecomprimeerde bijlage. Het profiel kan alleen op het apparaat worden herkend en geïnstalleerd als de bestanden niet gecomprimeerd zijn.

Configuratieprofielen via het web distribueren

U kunt configuratieprofielen via een website distribueren. Gebruikers kunnen het profiel vervolgens installeren door dit via Safari op hun apparaat te downloaden. U kunt de URL eenvoudig naar de gebruikers distribueren door het per sms te versturen.

Een configuratieprofiel exporteren

1 Klik op de knop 'Exporteer' (Mac) of 'Exporteren' (Windows) in de knoppenbalk van iPhone-configuratieprogramma.

Selecteer een beveiligingsoptie in het venster dat wordt weergegeven:

a 'Geen':Het bestand .mobileconfig wordt in platte tekst aangemaakt. Dit bestand kan op elk gewenst apparaat worden geïnstalleerd. Bepaalde inhoud in het bestand is onleesbaar gemaakt om ongewenst meekijken te voorkomen als het bestand wordt bekeken. Wanneer u het bestand op uw website plaatst, moet u er echter voor zorgen dat het bestand alleen toegankelijk is voor bevoegde gebruikers.

b 'Onderteken configuratieprofiel' (Mac) of 'Configuratieprofiel ondertekenen' (Windows): Het bestand .mobileconfig wordt ondertekend en wordt niet op een apparaat geïnstalleerd als het bestand is gewijzigd. Na de installatie kan het profiel alleen worden bijgewerkt door een profiel met dezelfde aanduiding die is ondertekend met hetzelfde exemplaar van iPhone-configuratieprogramma. Bepaalde gegevens in het profiel zijn onleesbaar gemaakt om ongewenst meekijken te voorkomen als het bestand wordt bekeken. Wanneer u het bestand op uw website plaatst, moet u er echter voor zorgen dat het bestand alleen toegankelijk is voor bevoegde gebruikers.

c 'Onderteken en codeer profiel' (Mac) of 'Profiel ondertekenen en coderen' (Windows): Het profiel wordt ondertekend zodat dit niet kan worden gewijzigd. Bovendien wordt de volledige inhoud van het profiel gecodeerd zodat het profiel niet kan worden bekeken en alleen op een specifiek apparaat kan worden geïnstalleerd. Voor elk apparaat dat u in de lijst 'Apparaten' selecteert, wordt een afzonderlijk .mobileconfig-bestand aangemaakt.

2 Klik op 'Exporteer' (Mac) of 'Exporteren' (Windows) en selecteer de locatie waar u de .mobileconfig-bestanden wilt bewaren.

De bestanden kunnen direct op uw website worden geplaatst. U mag het .mobileconfig-bestand niet comprimeren en de bestandsextensie niet wijzigen; als u dat wel doet, wordt het profiel niet door het apparaat herkend of geïnstalleerd.

Installatie van gedownloade configuratieprofielen door gebruikers

U dient uw gebruikers de URL te geven vanaf waar ze de profielen naar hun apparaat kunnen downloaden, of de profielen naar een e-mailaccount te sturen die de gebruikers vanaf hun apparaat kunnen benaderen voordat dit is voorzien van uw bedrijfsspecifieke gegevens.

Als een gebruiker het profiel vanaf het web downloadt of de bijlage opent met Mail, wordt het bestand aan de hand van de extensie '.mobileconfig' herkend als profiel en wordt de installatie gestart zodra de gebruiker op 'Installeer' tikt.

Tijdens de installatieprocedure wordt de gebruiker gevraagd om de benodigde gegevens in te voeren, zoals wachtwoorden die niet in het profiel zijn opgegeven, en eventuele andere gegevens die op grond van de instellingen nodig zijn.

Het apparaat haalt bovendien de Exchange ActiveSync-beleidsinstellingen van de server op en zal bij elke volgende verbinding controleren of er een nieuwe versie van de beleidsinstellingen is en die zo nodig ophalen. Als het apparaat of de Exchange ActiveSync-beleidsinstellingen een toegangscode vereisen, wordt de installatie alleen voltooid indien de gebruiker een code opgeeft die overeenkomt met de beleidsinstellingen.

Daarnaast moet de gebruiker de wachtwoorden opgeven die nodig zijn om gebruik te kunnen maken van de certificaten die in het profiel zijn opgenomen.

Als de installatie niet wordt voltooid, bijvoorbeeld omdat de Exchange-server niet bereikbaar was of omdat de gebruiker het proces heeft geannuleerd, blijven de gegevens die door de gebruiker waren ingevoerd, niet bewaard.

Mogelijk willen gebruikers het aantal dagen wijzigen waarvan gegevens met het apparaat worden gesynchroniseerd en de e-mailmappen wijzigen die (naast de postbus) worden gesynchroniseerd. De standaardwaarden voor deze opties zijn drie dagen en alle mappen. Gebruikers kunnen deze waarden wijzigen via 'Instellingen' > 'Mail, Contacten, Agenda' > [Naam Exchange-account].

Configuratieprofielen verwijderen en bijwerken

Bijgewerkte configuratieprofielen worden niet bij de gebruikers afgeleverd. Distribueer de bijgewerkte profielen naar de gebruikers zodat ze deze kunnen installeren. Zolang de profielaanduiding niet verandert en (indien ondertekend) is ondertekend met hetzelfde exemplaar van iPhone-configuratieprogramma, wordt het profiel op het apparaat vervangen door het nieuwe profiel.

Instellingen die door een configuratieprofiel zijn aangebracht, kunnen niet op het apparaat worden gewijzigd. Om een instelling te wijzigen, moet een bijgewerkt profiel worden geïnstalleerd. Als het profiel is ondertekend, kan het alleen worden vervangen door een profiel dat met hetzelfde exemplaar van iPhone-configuratieprogramma is ondertekend. In beide profielen moet de aanduiding gelijk zijn, zodat het bijgewerkte profiel als vervanging kan worden herkend. Zie “Algemeen” op pagina 34 voor meer informatie over de aanduiding.

Belangrijk: Wanneer een configuratieprofiel wordt verwijderd, gaan ook de bijbehorende beleidsinstellingen en alle gegevens van de Exchange-account die op het apparaat zijn bewaard, de VPN-instellingen, de certificaten en alle overige profielgegevens (waaronder de e-mailberichten) verloren.

Als in de payload 'Algemeen' van het profiel is opgegeven dat het profiel niet door de gebruiker kan worden verwijderd, wordt de knop 'Verwijder' niet weergegeven. Als in de instellingen is opgegeven dat het profiel kan worden verwijderd met een wachtwoord ter autorisatie, wordt de gebruiker gevraagd een wachtwoord in te voeren nadat op 'Verwijder' is getikt. Zie “Algemeen” op pagina 34 voor meer informatie over beveiligingsinstellingen voor profielen.

Apparaten handmatig configureren

3

Dit hoofdstuk bevat informatie over het handmatig configureren van de iPhone, iPod touch en iPad.

Als u de gebruikers geen profielbestanden voor automatische configuratie verstrekt, kunnen ze hun apparaten handmatig configureren. Bepaalde instellingen, zoals het toegangscodebeleid, kunnen alleen met een configuratieprofiel worden ingesteld.

VPN-instellingen

Om de VPN-instellingen te wijzigen, gaat u naar 'Instellingen' > 'Algemeen' > 'Netwerk' > 'VPN'.

Bij het configureren van VPN-instellingen wordt u om bepaalde gegevens gevraagd, afhankelijk van de respons die het apparaat van de VPN-server ontvangt. Zo wordt u bijvoorbeeld om een RSA SecurID-token gevraagd als dit voor de server vereist is.

U kunt alleen een VPN-verbinding op basis van certificaten configureren als de benodigde certificaten op het apparaat zijn geïnstalleerd. Zie “Identiteiten en rootcertificaten installeren” op pagina 60 voor meer informatie.

VPN op aanvraag kan niet op het apparaat worden geconfigureerd omdat u deze voorziening moet instellen met behulp van een configuratieprofiel. Zie “VPN op aanvraag” op pagina 38.

VPN-proxyinstellingen

U kunt ook één VPN-proxy opgeven voor alle configuraties. Om voor alle verbindingen één proxy te configureren, tikt u op 'Handmatig' en geeft u het adres, de poort en indien nodig de identiteitscontrole op. Als u voor het apparaat een bestand voor automatische proxyconfiguraties wilt opgeven, tikt u op 'Autom.' en geeft u de URL van het PACS-bestand op. Om een automatische proxyconfiguratie met behulp van WPAD op te geven, tikt u op 'Autom.'. Op het apparaat worden de WPAD-instellingen gezocht via DHCP en DNS. Zie “Meer informatie” aan het einde van dit hoofdstuk voor voorbeelden van PACS-bestanden en voor meer informatie over PACS.

Cisco IPSec-instellingen

Wanneer u het apparaat handmatig configureert voor Cisco IPSec VPN, verschijnt een scherm dat er ongeveer zo uitziet:

Hieronder wordt uitleg gegeven over de instellingen en de gegevens die u moet invoeren:

Veld	Beschrijving
Beschrijving	Een aanduiding voor deze groep instellingen.
Server	De DNS-naam of het IP-adres van de VPN-server waarmee verbinding moet worden gemaakt.
Account	De gebruikersnaam van de VPN-inlogaccount van de gebruiker. Voer hier niet de groepsnaam in.
Wachtwoord	De wachtzin van de VPN-inlogaccount van de gebruiker. Laat dit veld leeg bij identiteitscontrole op basis van RSA SecurID en CryptoCard of als u wilt dat de gebruiker bij elke verbindingspoging het wachtwoord handmatig invoert.
Gebruik certificaat	Deze optie is alleen beschikbaar als u een .p12- of .pfx-identiteit hebt geïnstalleerd die bestaat uit een certificaat dat geschikt is voor externe toegang en een private sleutel voor het certificaat. Wanneer 'Gebruik certificaat' is ingeschakeld, worden de velden 'Groepsnaam' en 'Geheim' vervangen door het veld 'Certificaat' waarin u kunt kiezen uit een lijst met geïnstalleerde identiteiten die compatibel zijn met VPN.
Groepsnaam	De naam van de groep waartoe de gebruiker behoort, zoals gedefinieerd op de VPN-server.
Geheim	Het gedeelde geheim van de groep. Dit is hetzelfde voor alle leden van de groep waartoe de gebruiker behoort. Dit is niet het wachtwoord van de gebruiker. Het geheim moet worden opgegeven om een verbinding tot stand te kunnen brengen.

PPTP-instellingen

Wanneer u het apparaat handmatig configureert voor PPTP VPN, verschijnt een scherm dat er ongeveer zo uitziet:

Hieronder wordt uitleg gegeven over de instellingen en de gegevens die u moet invoeren:

Veld	Beschrijving
Beschrijving	Een aanduiding voor deze groep instellingen.
Server	De DNS-naam of het IP-adres van de VPN-server waarmee verbinding moet worden gemaakt.
Account	De gebruikersnaam van de VPN-inlogaccount van de gebruiker.
RSA SecurID	Als u een RSA SecurID-token gebruikt, moet u deze optie inschakelen om ervoor te zorgen dat het veld 'Wachtwoord' wordt verborgen.
Wachtwoord	De wachtzin van de VPN-inlogaccount van de gebruiker.
Coderingsniveau	De standaardinstelling is 'Autom.'. Hierbij wordt het hoogst mogelijke coderingsniveau toegepast, te beginnen bij 128-bits, vervolgens 40-bits en tot slot 'Geen'. Bij 'Maximum' wordt uitsluitend 128-bits-codering gebruikt. Als u 'Geen' kiest, wordt de codering uitgeschakeld.
Stuur alle verkeer	Deze instelling is standaard ingeschakeld en zorgt ervoor dat al het netwerkverkeer via de VPN-verbinding wordt verstuurd. Schakel de instelling uit als u split-tunneling wilt gebruiken. Hierbij wordt alleen verkeer via de VPN-server verstuurd dat een server binnen het VPN-netwerk als bestemming heeft. Ander verkeer wordt direct naar het internet doorgestuurd.

L2TP-instellingen

Wanneer u het apparaat handmatig configureert voor L2TP VPN, verschijnt een scherm dat er ongeveer zo uitziet:

Hieronder wordt uitleg gegeven over de instellingen en de gegevens die u moet invoeren:

Veld	Beschrijving
Beschrijving	Een aanduiding voor deze groep instellingen.
Server	De DNS-naam of het IP-adres van de VPN-server waarmee verbinding moet worden gemaakt.
Account	De gebruikersnaam van de VPN-inlogaccount van de gebruiker.
Wachtwoord	Het wachtwoord van de VPN-inlogaccount van de gebruiker.
Geheim	Het gedeelde geheim (de vooraf gedeelde sleutel) voor de L2TP-account. Dit is voor alle LT2P-gebruikers gelijk.
Stuur alle verkeer	Deze instelling is standaard ingeschakeld en zorgt ervoor dat al het netwerkverkeer via de VPN-verbinding wordt verstuurd. Schakel de instelling uit als u split-tunneling wilt gebruiken. Hierbij wordt alleen verkeer via de VPN-server verstuurd dat een server binnen het VPN-netwerk als bestemming heeft. Ander verkeer wordt direct naar het internet doorgestuurd.

Wi-Fi-instellingen

Om de Wi-Fi-instellingen te wijzigen, tikt u achtereenvolgens op 'Instellingen' > 'Algemeen' > 'Netwerk' > 'Wi-Fi'. Als u een netwerk wilt toevoegen dat binnen het bereik ligt, kunt u het selecteren in de lijst met beschikbare netwerken. Als u een ander netwerk wilt toevoegen, tikt u op 'Anders'.

Controleer of uw netwerkinfrastructuur methoden voor identiteitscontrole en codering gebruikt die door de iPhone en iPod touch worden ondersteund. Zie “Netwerkbeveiliging” op pagina 11 voor specificaties. Zie “Identiteiten en rootcertificaten installeren” op pagina 60 voor informatie over de installatie van certificaten voor identiteitscontrole.

Exchange-instellingen

Per apparaat kunt u slechts één Exchange-account instellen. Om een Exchange-account toe te voegen, tikt u achtereenvolgens op 'Instellingen' > 'Mail, Contacten, Agenda' > 'Voeg account toe'. Tik in het scherm 'Voeg account toe' op 'Microsoft Exchange'.

Hieronder wordt uitleg gegeven over de instellingen en de gegevens die u moet invoeren bij het handmatig configureren van het apparaat voor Exchange:

Veld	Beschrijving
E-mail	Het volledige e-mailadres van de gebruiker.
Domein	Het domein van de Exchange-account van de gebruiker.
Gebruikersnaam	De gebruikersnaam van de Exchange-account van de gebruiker.
Wachtwoord	Het wachtwoord van de Exchange-account van de gebruiker.
Beschrijving	Een aanduiding voor deze account.

De iPhone, iPod touch en iPad bieden ondersteuning voor de Autodiscover-voorziening van Microsoft. Deze voorziening bepaalt op basis van uw gebruikersnaam en wachtwoord wat het adres is van de Exchange-frontendserver. Als dit adres niet kan worden vastgesteld, wordt u gevraagd om het in te voeren.

Als uw Exchange-server voor verbindingen gebruikmaakt van een andere poort dan poort 443, geeft u het juiste poortnummer op in het veld 'Server'. Gebruik daarbij de notatie exchange.voorbeeld.com:poortnummer.

Als de Exchange-account is geconfigureerd, wordt het toegangscodebeleid van de server toegepast. Als de huidige toegangscode van de gebruiker niet aan het Exchange ActiveSync-beleid voldoet, wordt de gebruiker gevraagd de toegangscode te wijzigen. Het apparaat kan alleen verbinding maken met de Exchange-server als de gebruiker een geldige toegangscode heeft ingesteld.

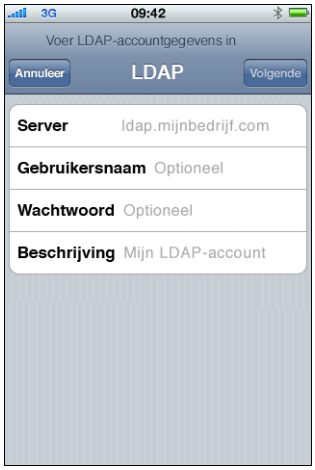
Het apparaat vraagt vervolgens of u uw gegevens direct met de Exchange-server wilt synchroniseren. U kunt de synchronisatie van agenda- en contactgegevens op dat moment overslaan en deze later alsnog inschakelen via 'Instellingen' > 'Mail, Contacten, Agenda'. Standaard worden nieuwe gegevens automatisch door Exchange ActiveSync op uw apparaat afgeleverd zodra ze op de server binnenkomen. Als u liever een schema instelt voor het ophalen van nieuwe gegevens of nieuwe gegevens alleen handmatig wilt ophalen, wijzigt u de instellingen via 'Instellingen' > 'Mail, Contacten, Agenda' > 'Nieuwe gegevens'.

Als u het aantal dagen wilt wijzigen waarvan e-mailberichten met het apparaat worden gesynchroniseerd, tikt u op 'Instellingen' > 'Mail, Contacten, Agenda' en selecteert u de Exchange-account. Daarnaast kunt u aangeven welke mappen (naast de postbus) worden opgenomen in de levering van push-e-mail.

Om de instelling voor agendagegevens te wijzigen, tikt u op 'Instellingen' > 'Mail, Contacten, Agenda' > 'Synchroniseer'.

LDAP-instellingen

U kunt via de iPhone, iPod touch en iPad de contactgegevens op LDAP-adreslijstservers opzoeken. Om een LDAP-server toe te voegen, tikt u op 'Instellingen' > 'Mail, Contacten, Agenda' > 'Voeg account toe' > 'Anders'. Tik vervolgens op 'Voeg LDAP-account toe'.



Voer het adres en indien vereist de gebruikersnaam en het wachtwoord van de LDAP-server in en tik op 'Volgende'. Als de server bereikbaar is en de standaardzoekinstellingen aan het apparaat worden verstrekt, worden deze instellingen gebruikt.

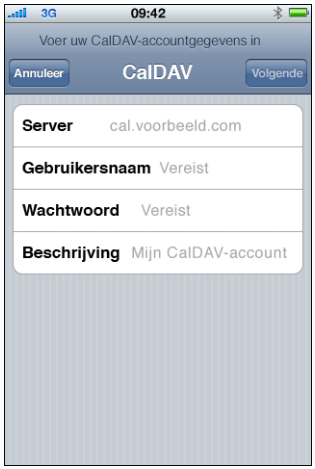
Voor het zoekbereik worden de volgende instellingen gebruikt:

Instelling voor zoekbereik	Beschrijving
Basis	Hiermee wordt alleen het basisobject doorzocht.
Eén niveau	Hiermee worden objecten één niveau onder het basisobject doorzocht. Het basisobject zelf wordt niet doorzocht.
Subhiërarchie	Hiermee worden het basisobject en de volledige hiërarchie met alle objecten vanaf het basisobject doorzocht.

U kunt voor elke server meerdere sets met zoekinstellingen opgeven.

CalDAV

De groepsagenda's en groepsactiviteiten worden op de iPhone, iPod touch en iPad verstrekt via CalDAV-agendaservers. Om een CalDAV-server toe te voegen, tikt u op 'Instellingen' > 'Mail, Contacten, Agenda' > 'Voeg account toe' > 'Anders'. Tik vervolgens op 'Voeg CalDAV-account toe'.



Voer het adres en indien vereist de gebruikersnaam en het wachtwoord van de CalDAV-server in en tik op 'Volgende'. Zodra de verbinding met de server tot stand is gebracht, verschijnen extra velden waarin u meer opties kunt instellen.

Instellingen voor agenda-abonnement

U kunt alleen-lezenagenda's met bedrijfsactiviteiten als feestdagen of planningen voor speciale activiteiten toevoegen. Om een agenda toe te voegen, tikt u op 'Instellingen' > 'Mail, Contacten, Agenda' > 'Voeg account toe' > 'Anders' en tikt u vervolgens op 'Voeg agenda-abonnement toe'.

Voer de URL voor een iCalendar-bestand (.ics) in en indien vereist de gebruikersnaam en het wachtwoord, en tik vervolgens op 'Bewaar'. U kunt ook opgeven of eventuele herinneringen die in de agenda zijn ingesteld, moeten worden verwijderd wanneer de agenda aan het apparaat wordt toegevoegd.

Naast het handmatig toevoegen van agenda-abonnementen kunt u gebruikers een webcal://- URL (of een HTTP://- koppeling naar een .ics-bestand) versturen. Wanneer de gebruiker op de koppeling tikt, wordt gevraagd of de koppeling als agenda-abonnement moet worden toegevoegd.

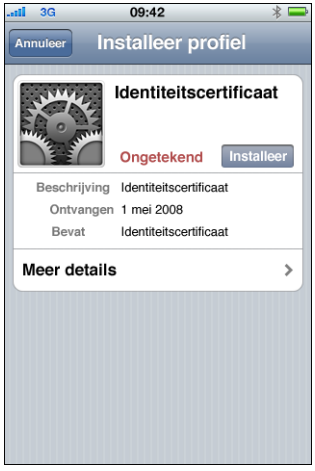
Identiteiten en rootcertificaten installeren

Als u certificaten niet via profielen distribueert, kunnen gebruikers ze handmatig installeren door ze met de iPhone of iPod touch vanaf een website te downloaden of door een bijlage in een e-mailbericht te openen. Het apparaat herkent certificaten met de volgende MIME-typen en bestandsextensies:

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

Zie “Certificaten en identiteiten” op pagina 12 voor meer informatie over ondersteunde structuren en andere vereisten.

Als een certificaat of identiteit naar het apparaat is gedownload, verschijnt het scherm 'Installeer profiel'. De beschrijving geeft aan om welk type het gaat: identiteitscertificaat of certificaatautoriteit. Tik op 'Installeer' om het certificaat te installeren. Als het gaat om een identiteitscertificaat, moet u het wachtwoord van het certificaat invoeren.



Om een geïnstalleerd certificaat te bekijken of te verwijderen, tikt u op 'Instellingen' > 'Algemeen' > 'Profiel'. Als u een certificaat verwijdert dat vereist is voor toegang tot een account of netwerk, kan het apparaat hier geen verbinding meer mee maken.

Extra e-mailaccounts

U kunt slechts één Exchange-account instellen. U kunt echter wel meerdere POP- en IMAP-accounts toevoegen. Deze kunt u bijvoorbeeld gebruiken voor toegang tot e-mail op een Lotus Notes- of Novell Groupwise-mailserver. Hiervoor tikt u op 'Instellingen' > 'Accounts' > 'Mail, Contacten, Agenda' > 'Voeg account toe' > 'Anders'. Raadpleeg de *iPhone-gebruikershandleiding, iPod touch-gebruikershandleiding,* of de *iPad-gebruikershandleiding* voor meer informatie over het toevoegen van een IMAP-account.

Profielen bijwerken en verwijderen

Zie “Configuratieprofielen verwijderen en bijwerken” op pagina 48 voor informatie over de manier waarop gebruikers configuratieprofielen kunnen bijwerken of verwijderen.

Zie “Programma's implementeren” op pagina 70 voor informatie over het installeren van voorzieningenprofielen voor distributie.

Meer informatie

Raadpleeg de volgende informatiebronnen voor informatie over de structuur en de functie van bestanden voor automatische proxyconfiguratie die door de VPN-proxyinstellingen worden gebruikt:

- PAC (Proxy Auto-Config) op http://en.wikipedia.org/wiki/Proxy_auto-config
- Web Proxy Autodiscovery Protocol op http://en.wikipedia.org/wiki/Wpad
- Microsoft TechNet “Using Automatic Configuration, Automatic Proxy, and Automatic Detection” op http://technet.microsoft.com/en-us/library/dd361918.aspx

Er is divers videomateriaal beschikbaar, te bekijken in een standaardwebbrowser, waarin uitleg wordt gegeven over het configureren van de iPhone, iPod touch en iPad en het gebruik van de verschillende functies:

- De iPhone-rondleiding op www.apple.com/nl/iphone/guidedtour/
- De iPod touch-rondleiding op www.apple.com/nl/ipodtouch/guidedtour/
- De iPad-rondleiding op www.apple.com/ipad/guided-tours/
- De iPhone-ondersteuningspagina op www.apple.com/nl/support/iphone/
- De iPod touch-ondersteuningspagina op www.apple.com/nl/support/ipodtouch/
- De iPad-ondersteuningspagina op www.apple.com/nl/support/ipad/

Er is voor beide apparaten ook een gebruikershandleiding (pdf-bestand) beschikbaar met extra tips en instructies:

- De *iPhone-gebruikershandleiding* op http://manuals.info.apple.com/nl_NL/iPhone_Gebruikershandleiding.pdf

- De *iPod touch-gebruikershandleiding* op http://manuals.info.apple.com/nl_NL/iPod_touch_2.0_Gebruikershandleiding.pdf
- De *iPad-gebruikershandleiding* op: http://manuals.info.apple.com/nl_NL/iPad_Gebruikershandleiding.pdf

iTunes implementeren

4

Met iTunes kunt u muziek en video's synchroniseren, programma's installeren en nog veel meer.

Dit hoofdstuk bevat informatie over het implementeren van iTunes en bedrijfsprogramma's en over de instellingen en beperkingen die u kunt toepassen.

Alle typen gegevens (muziek, media, enzovoort) op de iPhone, iPod touch en iPad kunnen slechts met één computer tegelijk worden gesynchroniseerd. U kunt bijvoorbeeld muziek met een desktopcomputer en bladwijzers met een draagbare computer synchroniseren door de synchronisatieopties in iTunes op beide computers op de juiste manier in te stellen. Raadpleeg iTunes Help (beschikbaar in het Help-menu wanneer iTunes actief is) voor meer informatie over de synchronisatieopties.

iTunes installeren

Voor de installatie van iTunes worden de standaardinstallatieprogramma's van de Mac en Windows gebruikt. U kunt de nieuwste versie en een overzicht van de systeemvereisten downloaden vanaf www.itunes.com/nl.

Voor informatie over de licentievereisten voor de distributie van iTunes gaat u naar: http://developer.apple.com/softwarelicensing/agreements/itunes.html

iTunes op Windows-computers installeren

Wanneer u iTunes op Windows-computers installeert, wordt standaard ook de nieuwste versie van QuickTime, Bonjour en Apple Software-update geïnstalleerd. U kunt deze onderdelen weglaten door parameters aan het iTunes-installatieprogramma door te geven of door alleen de onderdelen die u wilt installeren op de computers van de gebruikers te "pushen".

iTunes op Windows-computers installeren met 'iTunesSetup.exe'

Als u iTunes op de standaardmanier wilt installeren maar enkele onderdelen wilt weglaten, kunt u via de commandoregel eigenschappen aan 'iTunesSetup.exe' doorgeven.

Eigenschap	Betekenis
NO_AMDS=1	Apple Mobile Device Services niet installeren. iTunes heeft dit onderdeel nodig voor het synchroniseren en beheren van mobiele apparaten.
NO_ASUW=1	Apple Software-update voor Windows niet installeren. Met dit programma worden gebruikers op de hoogte gesteld van nieuwe versies van Apple software.
NO_BONJOUR=1	Bonjour niet installeren. Met Bonjour worden printers, gedeelde iTunes-bibliotheken en andere voorzieningen in het netwerk automatisch gedetecteerd, zonder dat deze hoeven te worden geconfigureerd.
NO_QUICKTIME=1	QuickTime niet installeren. Dit onderdeel is nodig om iTunes te kunnen gebruiken. Laat QuickTime alleen weg als u zeker weet dat de nieuwste versie al op de clientcomputer is geïnstalleerd.

Een stille installatie uitvoeren op Windows-computers

Om een stille installatie van iTunes uit te voeren, extraheert u de afzonderlijke .msi-bestanden uit 'iTunesSetup.exe' en pusht u de bestanden vervolgens naar de clientcomputers.

.msi-bestanden uit 'iTunesSetup.exe' extraheren

1. Voer 'iTunesSetup.exe' uit.
2. Open *%temp%* en zoek een map met de naam 'IXP*nnn*.TMP'. Hierbij is *%temp%* uw map voor tijdelijke bestanden en *nnn* een willekeurig getal van drie cijfers. In Windows XP bevindt de map voor tijdelijke bestanden zich doorgaans in opstartschijf:\Documents and Settings\[naam gebruiker]\Local Settings\Temp\. In Windows Vista bevindt de map voor tijdelijke bestanden zich doorgaans in \Users\[naam gebruiker]\AppData\Local\Temp\.
3. Kopieer de .msi-bestanden in deze map naar een andere locatie.
4. Stop het installatieprogramma dat u met 'iTunesSetup.exe' hebt gestart.

Gebruik vervolgens Groepsbeleidsobjecteditor in de Microsoft Management Console om de .msi-bestanden aan een beleid voor computerconfiguratie toe te voegen. Zorg ervoor dat u de configuratie aan het onderdeel 'Computerconfiguratie' toevoegt en niet aan het onderdeel 'Gebruikersconfiguratie'.

Belangrijk: Voor iTunes zijn QuickTime en Apple Application Support vereist. Apple Application Support moet zijn geïnstalleerd voordat u iTunes installeert. Om een iPhone, iPad of iPod touch met iTunes te kunnen gebruiken, is Apple Mobile Device Services (AMDS) vereist.

Voordat u de .msi-bestanden pusht, moet u aangeven welke gelokaliseerde versies van iTunes u wilt installeren. Hiervoor opent u het .msi-bestand in het ORCA-programma. Dit programma wordt samen met de Windows-SDK (in de map in bin\) geïnstalleerd als Orca.msi. Vervolgens wijzigt u de overzichtsgegevensstroom en verwijdert u de talen die u niet wilt installeren. (De landinstelling-ID 'ID1033' staat voor Engels.) U kunt ook Groepsbeleidsobjecteditor gebruiken om de implementatie-eigenschappen van de .msi-bestanden te wijzigen en de taal te negeren.

iTunes op de Mac installeren

Op Mac-computers is iTunes standaard al geïnstalleerd. U kunt de nieuwste versie van iTunes downloaden vanaf www.itunes.com/nl. Om iTunes naar Mac-clients te pushen, kunt u Workgroup Manager gebruiken, een beheerprogramma dat onderdeel is van Mac OS X Server.

Apparaten snel activeren met iTunes

Voordat een nieuwe iPhone, iPod touch of iPad kan worden gebruikt, moet het apparaat worden geactiveerd door het aan te sluiten op een computer waarop iTunes actief is. Normaliter vraagt iTunes na de activering of u het apparaat met de computer wilt synchroniseren. Om dit te vermijden wanneer u een apparaat voor iemand anders configureert, schakelt u de alleen-activerenmodus in. Als deze modus is ingeschakeld, wordt het apparaat automatisch uit iTunes verwijderd zodra het is geactiveerd. Het apparaat kan vervolgens verder worden geconfigureerd, maar bevat geen media of gegevens.

De alleen-activerenmodus inschakelen in Mac OS X

1. Zorg dat iTunes niet actief is en open vervolgens Terminal.
2. Voer in Terminal een commando in:
   - Alleen-activerenmodus inschakelen:

     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 1
     ```
   - Alleen-activerenmodus uitschakelen:

     ```
     defaults delete com.apple.iTunes StoreActivationMode
     ```

Zie “Alleen-activerenmodus gebruiken” hieronder om een apparaat te activeren.

Alleen-activerenmodus inschakelen in Windows

1. Zorg dat iTunes niet actief is en open vervolgens een commandoregelvenster.
2. Voer een commando in:
   - Alleen-activerenmodus inschakelen:

     ```
     "C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 1
     ```
   - Alleen-activerenmodus uitschakelen:

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

U kunt ook een snelkoppeling aanmaken of de bestaande iTunes-snelkoppeling wijzigen en deze commando's deel laten uitmaken van de snelkoppeling zodat u de alleen-activerenmodus snel kunt in- en uitschakelen.

Om te controleren of de alleen-activerenmodus voor iTunes is ingeschakeld, kiest u 'iTunes' > 'Over iTunes' (Mac) of 'Help' > 'Info iTunes' (Windows) en kijkt u of de tekst "alleen-activerenmodus" onder de iTunes-versie en de buildinformatie wordt weergegeven.

Alleen-activerenmodus gebruiken

Zorg ervoor dat u de alleen-activerenmodus hebt ingeschakeld, zoals hierboven beschreven, en voer vervolgens deze stappen uit.

1. Als u een iPhone activeert, plaatst u een geactiveerde simkaart in de iPhone. Gebruik de simkaartverwijdertool of een rechtgebogen paperclip om de simhouder te verwijderen. Raadpleeg de *iPhone-gebruikershandleiding* voor meer informatie.
2. Sluit de iPhone, iPod touch of iPad op de computer aan. De computer moet verbonden zijn met het internet om het apparaat te kunnen activeren.

   iTunes wordt zo nodig geopend en het apparaat wordt geactiveerd. Er verschijnt een melding zodra het apparaat is geactiveerd.
3. Koppel het apparaat los.

   U kunt onmiddellijk extra apparaten aansluiten en activeren. iTunes voert met geen enkel apparaat een synchronisatie uit wanneer de alleen-activerenmodus is ingeschakeld. Vergeet dus niet om de alleen-activerenmodus weer uit te schakelen wanneer u iTunes wilt gebruiken voor het synchroniseren van apparaten.

Beperkingen instellen voor iTunes

U kunt iTunes zo instellen dat gebruikers bepaalde functies niet kunnen gebruiken. Dit wordt ook wel ouderlijk toezicht genoemd. U kunt beperkingen instellen voor de volgende functies:

- Automatisch of via een opdracht van de gebruiker zoeken naar nieuwe versies van iTunes en software-updates voor apparaten
- Suggesties van Genius weergeven tijdens het zoeken of afspelen van mediamateriaal
- Automatisch synchroniseren wanneer apparaten zijn aangesloten
- Albumillustraties downloaden
- Plugins voor visuele effecten gebruiken
- Een URL voor streaming media invoeren
- Automatisch zoeken naar Apple TV-systemen
- Nieuwe apparaten bij Apple registreren
- Abonneren op podcasts
- Internetradio beluisteren

- Toegang tot de iTunes Store
- De bibliotheek delen met lokale netwerkcomputers waarop iTunes is geïnstalleerd
- iTunes-materiaal afspelen dat als expliciet is aangemerkt
- Films afspelen
- Tv-programma's afspelen

Beperkingen voor iTunes instellen onder Mac OS X

Onder Mac OS X stelt u toegangsbeperkingen in door middel van sleutels in een plist-bestand. U kunt voor elke gebruiker sleutelwaarden instellen voor de bovengenoemde functies door het bestand ~/Bibliotheek/Preferences/com.apple.iTunes.plist te bewerken met Workgroup Manager, een beheerprogramma dat onderdeel is van Mac OS X Server.

Zie voor instructies het Apple Support-artikel op:
http://docs.info.apple.com/article.html?artnum=303099-nl

Beperkingen voor iTunes instellen onder Windows

Onder Windows stelt u toegangsbeperkingen in door registerwaarden in te stellen in een van de volgende registersleutels:

Windows XP en 32-bits Windows Vista:

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

64-bits Windows Vista:

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

Zie voor informatie over de iTunes-registerwaarden het Apple Support-artikel op:
http://support.apple.com/kb/HT2102?viewlocale=nl_NL

Zie voor algemene informatie over bewerking van het Windows-register het artikel over Microsoft Help en ondersteuning op http://support.microsoft.com/kb/136393.

iTunes en iPhone OS handmatig bijwerken

Als u in iTunes het automatisch en door de gebruiker geïnitieerde zoeken naar software-updates uitschakelt, moet u de gebruikers software-updates verstrekken, zodat ze deze handmatig kunnen installeren.

Voor het bijwerken van iTunes raadpleegt u de instructies voor installatie en implementatie eerder in dit document. De procedure is dezelfde die u voor de distributie van iTunes aan uw gebruikers hebt gevolgd.

Voor het bijwerken van iPhone OS voert u onderstaande procedure uit:

1. Op een computer waarop het zoeken naar software-updates niet is uitgeschakeld in iTunes, kunt u de bijgewerkte software via iTunes downloaden. Selecteer hiervoor een aangesloten apparaat in iTunes, klik op de tab 'Samenvatting' en klik vervolgens op de knop 'Zoek naar update' (Mac) of 'Update zoeken' (Windows).
2. Als het downloaden is voltooid, kopieert u het updater-bestand (.ipsw) vanuit de volgende locatie:
   - *Mac OS X:* ~/Library/iTunes/iPhone Software Updates/
   - *Windows XP:* opstartschijf:\Documents and Settings\gebruiker\Application Data\Apple Computer\iTunes\iPhone Software Updates\
3. Verstrek het .ipsw-bestand aan de gebruikers of maak het via het netwerk beschikbaar.
4. Vertel de gebruikers dat ze met iTunes een reservekopie moeten maken van de gegevens op het apparaat voordat ze de update toepassen. Bij handmatige updates wordt door iTunes niet automatisch een reservekopie gemaakt voordat de installatie wordt uitgevoerd. Om een nieuwe reservekopie te maken, klikt u met de rechtermuisknop (Windows) of met Control ingedrukt (Mac) op het apparaat in de navigatiekolom van iTunes. Kies vervolgens 'Reservekopie' uit het contextuele menu.
5. De gebruikers kunnen de update installeren door het apparaat op de computer met iTunes aan te sluiten en vervolgens de tab 'Samenvatting' voor het desbetreffende apparaat te selecteren. Daarna moeten ze de Option-toets (Mac) of de Shift-toets (Windows) ingedrukt houden en op de knop 'Zoek naar update' (Mac) of 'Update zoeken' (Windows) klikken.
6. Er verschijnt een venster waarin een bestand kan worden geselecteerd. De gebruikers moeten het .ipsw-bestand selecteren en vervolgens op 'Open' (Mac) of 'Openen' (Windows) klikken om de update uit te voeren.

Een reservekopie maken van een apparaat met iTunes

Als de iPhone, iPod touch of iPad is gesynchroniseerd met iTunes, wordt op de computer automatisch een reservekopie van de apparaatinstellingen gemaakt. Programma's die u via de App Store hebt gekocht, worden naar de bibliotheek in iTunes gekopieerd.

Van programma's die u zelf hebt ontwikkeld en naar gebruikers hebt gedistribueerd met behulp van profielen voor bedrijfsdistributie, wordt geen reservekopie gemaakt of naar de computer van de gebruiker overgebracht. De reservekopie van de gegevens op het apparaat bevat echter wel gegevensbestanden die door uw programma's zijn gemaakt.

U kunt reservekopieën van de gegevens op het apparaat gecodeerd bewaren door de optie voor het coderen van reservekopieën in het paneel 'Samenvatting' voor het apparaat in iTunes te selecteren. Bestanden worden gecodeerd met AES256. De sleutel wordt veilig bewaard in de sleutelhanger van iPhone OS.

Belangrijk: Als voor het apparaat waarvan u een reservekopie van de gegevens hebt gemaakt, gecodeerde profielen bestaan, moet de gebruiker in iTunes de optie voor codering van reservekopieën inschakelen.

Programma's implementeren

5

U kunt programma's voor de iPhone, iPod touch en iPad binnen uw bedrijf distribueren.

iPhone OS-programma's die u zelf hebt ontwikkeld, distribueert u aan de gebruikers waarna zij de programma's via iTunes kunnen installeren.

Programma's uit de online App Store zijn zonder extra stappen direct op de iPhone, iPod touch en iPad te gebruiken. Als u een programma hebt ontwikkeld dat u zelf wilt distribueren, moet u het programma digitaal ondertekenen met een door Apple uitgegeven certificaat. Ook moet u de gebruikers een voorzieningenprofiel voor distributie verstrekken om gebruik van het programma op hun iPhone of iPod touch mogelijk te maken.

De procedure voor het implementeren van uw eigen programma's is als volgt:

- Meld u bij Apple aan voor het ontwikkelaarsprogramma voor bedrijven.
- Onderteken uw programma's met uw certificaat.
- Maak een voorzieningenprofiel voor bedrijfsdistributie aan om gebruik van de ondertekende programma's op de apparaten mogelijk te maken.
- Stuur de programma's en het voorzieningenprofiel voor bedrijfsdistributie naar de computers van de gebruikers.
- Geef de gebruikers instructies voor het installeren van de programma's en het profiel via iTunes.

De verschillende stappen worden hieronder nader uitgelegd.

Aanmelden voor het ontwikkelen van programma's

Om aangepaste programma's voor iPhone OS te kunnen ontwikkelen en distribueren, moet u zich eerst aanmelden voor het iPhone Enterprise Developer Program op www.apple.com/nl/developer/.

Na aanmelding ontvangt u instructies om uw programma's geschikt te maken voor de apparaten.

Programma's ondertekenen

Programma's die u wilt distribueren, moeten met uw distributiecertificaat zijn ondertekend. In het iPhone Developer Center op http://developer.apple.com/iphone vindt u instructies voor het verkrijgen en gebruiken van dergelijke certificaten.

Het voorzieningenprofiel voor distributie aanmaken

Een voorzieningenprofiel voor distributie maakt het mogelijk programma's te ontwikkelen die anderen in uw bedrijf op hun apparaat kunnen gebruiken. Om een voorzieningenprofiel voor bedrijfsdistributie aan te maken voor een specifiek programma, of voor meerdere programma's, geeft u de AppID op waarvoor het profiel bedoeld is. Als een gebruiker wel over een bepaald programma beschikt, maar geen profiel heeft dat gebruik van het programma toestaat, kan hij of zij het programma niet gebruiken.

De speciaal aangewezen Team Agent voor uw bedrijf kan voorzieningenprofielen voor distributie aanmaken via de Enterprise Program Portal op http://developer.apple.com/iphone. Zie de instructies op de website.

Als u het voorzieningenprofiel voor bedrijfsdistributie hebt aangemaakt, kunt u het .mobileprovision-bestand downloaden en het profiel en het programma vervolgens op een veilige manier distribueren.

Voorzieningenprofielen installeren via iTunes

Vanaf de computer van de gebruiker worden voorzieningenprofielen automatisch door iTunes geïnstalleerd als de profielen in de mappen staan die in dit gedeelte worden beschreven. Als deze mappen niet bestaan, maakt u ze aan en gebruikt u hiervoor de namen die hieronder worden vermeld.

Mac OS X

- ~/Bibliotheek/MobileDevice/Provisioning Profiles/
- /Bibliotheek/MobileDevice/Provisioning Profiles/
- Het pad dat is opgegeven in de sleutel 'ProvisioningProfilesPath' in ~/Bibliotheek/Preferences/com.apple.itunes

Windows XP

- Opstartschijf:\Documents and Settings\gebruikersnaam\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- *Opstartschijf*:\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- Het pad dat is opgegeven in de registerwaarde 'ProvisioningProfilesPath' in de HKCU- of HKLM-registersleutel 'SOFTWARE\Apple Computer, Inc\iTunes'

Windows Vista

- Opstartschijf: \Users\gebruikersnaam\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *Opstartschijf*: \ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- Het pad dat is opgegeven in de registerwaarde 'ProvisioningProfilesPath' in de HKCU- of HKLM-registersleutel 'SOFTWARE\Apple Computer, Inc\iTunes'

Voorzieningenprofielen die op deze locaties staan, worden automatisch door iTunes geïnstalleerd op apparaten die met iTunes worden gesynchroniseerd. Geïnstalleerde voorzieningenprofielen zijn op het apparaat te bekijken via 'Instellingen' > 'Algemeen' > 'Profielen'.

U kunt ook het .mobileprovision-bestand distribueren. Als gebruikers dit bestand naar het programmasymbool van iTunes slepen, wordt het bestand naar de juiste locatie gekopieerd (een van de hierboven genoemde locaties).

Voorzieningenprofielen installeren met iPhone-configuratieprogramma

U kunt iPhone-configuratieprogramma gebruiken om voorzieningenprofielen op aangesloten apparaten te installeren. Volg hiervoor de onderstaande stappen:

1. Open iPhone-configuratieprogramma en kies 'Archief' > 'Voeg toe aan bibliotheek' (Mac) of 'Bestand' > 'Aan bibliotheek toevoegen' (Windows). Selecteer vervolgens het voorzieningenprofiel dat u wilt installeren.

   Het profiel wordt toegevoegd aan iPhone-configuratieprogramma en kan worden bekeken door in de bibliotheek de categorie 'Voorzieningenprofielen' te selecteren.
2. Selecteer een apparaat in de lijst 'Verbonden apparaten'.
3. Klik op de tab 'Voorzieningenprofielen'.
4. Selecteer het voorzieningenprofiel in de lijst en klik vervolgens op de bijbehorende knop 'Installeer' (Mac) of 'Installeren' (Windows).

Programma's installeren via iTunes

Gebruikers moeten de programma's via iTunes op hun apparaat installeren. Distribueer de programma's op een veilige manier en geef gebruikers de volgende instructies:

1. Open iTunes, kies 'Archief' > 'Voeg toe aan bibliotheek' (Mac) of 'Bestand' > 'Aan bibliotheek toevoegen' (Windows) en selecteer het gedistribueerde programma (.app).

   U kunt het .app-bestand ook naar het programmasymbool van iTunes slepen.
2. Sluit een apparaat op de computer aan en selecteer het vervolgens in de lijst 'Apparaten' in iTunes.
3. Klik op de tab 'Programma's' en selecteer het programma in de lijst.

4 Klik op 'Pas toe' (Mac) of 'Toepassen' (Windows) om het programma te installeren inclusief alle voorzieningenprofielen voor distributie vanuit de mappen die beschreven staan in het gedeelte “Voorzieningenprofielen installeren via iTunes” op pagina 71.

Programma's installeren met iPhone-configuratieprogramma

U kunt iPhone-configuratieprogramma gebruiken om programma's op aangesloten apparaten te installeren. Volg hiervoor de onderstaande stappen:

1 Open iPhone-configuratieprogramma en kies 'Archief' > 'Voeg toe aan bibliotheek' (Mac) of 'Bestand' > 'Aan bibliotheek toevoegen' (Windows). Selecteer vervolgens het voorzieningenprofiel dat u wilt installeren.

   Het programma wordt toegevoegd aan iPhone-configuratieprogramma en kan worden bekeken door in de bibliotheek de categorie 'Programma's' te selecteren.

2 Selecteer een apparaat in de lijst 'Verbonden apparaten'.

3 Klik op de tab 'Programma's'.

4 Selecteer het programma in de lijst en klik vervolgens op de bijbehorende knop 'Installeer' (Mac) of 'Installeren' (Windows).

Werken met bedrijfsprogramma's

Wanneer een gebruiker een programma start dat niet door Apple is ondertekend, zoekt het apparaat een voorzieningenprofiel voor distributie dat gebruik van het programma toestaat. Als er geen profiel is gevonden, kan het programma niet worden geopend.

Een bedrijfsprogramma uitschakelen

Als u een bedrijfsprogramma dat intern wordt gebruikt wilt uitschakelen, kunt u de identiteit intrekken waarmee het voorzieningenprofiel voor distributie is ondertekend. Het programma kan dan niet meer worden geïnstalleerd. Als het programma al is geïnstalleerd, kan het niet meer worden geopend.

Meer informatie

Voor meer informatie over het ontwikkelen van programma's en het aanmaken van voorzieningenprofielen raadpleegt u:

- iPhone Developer Center op http://developer.apple.com/iphone

Configuratie van de Cisco VPN-server

Deze bijlage bevat richtlijnen voor het configureren van de Cisco VPN-server voor gebruik met de iPhone, iPod touch en iPad.

Ondersteunde Cisco-platforms

iPhone OS ondersteunt Cisco ASA 5500 Security Appliances en PIX Firewalls die zijn geconfigureerd met softwareversie 7.2.x of hoger. De meest recente 8.0x-softwarerelease (of hoger) wordt aanbevolen. Daarnaast biedt iPhone OS ondersteuning voor Cisco IOS VPN-routers met IOS-versie 12.4(15)T of hoger. De VPN 3000 Series Concentrators bieden geen ondersteuning voor de VPN-voorzieningen op de iPhone.

Methoden voor identiteitscontrole

Voor iPhone OS kunnen de volgende methoden voor identiteitscontrole worden gebruikt:

- IPsec-identiteitscontrole op basis van een vooraf gedeelde sleutel met gebruikerscontrole via xauth;
- client- en servercertificaten voor IPsec-identiteitscontrole met optionele gebruikerscontrole via xauth;
- hybride identiteitscontrole waarbij de server een certificaat verstrekt en de client een vooraf gedeelde sleutel verstrekt voor IPsec-identiteitscontrole (gebruikerscontrole via xauth is vereist);
- voor gebruikerscontrole wordt xauth gebruikt op basis van een van de volgende methoden:
  - Gebruikersnaam met wachtwoord
  - RSA SecurID
  - CryptoCard

Identiteitscontrolegroepen

Het Cisco Unity-protocol gebruikt identiteitscontrolegroepen om gebruikers te groeperen op basis van gemeenschappelijke parameters voor onder andere identiteitscontrole. U moet een identiteitscontrolegroep aanmaken voor gebruikers van iPhone OS-apparaten. Voor hybride identiteitscontrole en controle op basis van een vooraf gedeelde sleutel moet bij het configureren van de groepsnaam op het apparaat het gedeelde geheim van de groep (de vooraf gedeelde sleutel) als groepswachtwoord worden ingesteld.

Voor identiteitscontrole op basis van certificaten wordt geen gedeeld geheim gebruikt en wordt de identiteit van de gebruikersgroep vastgesteld op basis van velden in het certificaat. U kunt de Cisco-serverinstellingen gebruiken om velden in een certificaat aan gebruikersgroepen te koppelen.

Certificaten

Bij het configureren en installeren van certificaten is het volgende van belang:

- In het identiteitscertificaat van de server moet in het SubjectAltName-veld de DNS-naam en/of het IP-adres van de server zijn ingevuld. Op basis van deze informatie controleert het apparaat of het certificaat bij de server hoort. U kunt jokertekens gebruiken voor de SubjectAltName, zoals 'vpn.*.mijnbedrijf.com', zodat de naam op meerdere servers van toepassing is en er meer flexibiliteit is. Als er geen SubjectAltName wordt opgegeven, kan de DNS-naam in het gewone naamveld worden ingevuld.
- Op het apparaat moet het certificaat zijn geïnstalleerd van de certificaatautoriteit die het servercertificaat heeft ondertekend. Als dit geen rootcertificaat is, moet u de rest van de vertrouwensketen installeren om ervoor te zorgen dat dit certificaat wordt vertrouwd.
- Bij gebruik van clientcertificaten moet u ervoor zorgen dat op de VPN-server het certificaat is geïnstalleerd van de vertrouwde certificaatautoriteit die het clientcertificaat heeft ondertekend.
- De certificaten en certificaatautoriteiten moeten geldig zijn (en dus niet verlopen).
- Het versturen van certificaatketens via de server wordt niet ondersteund en moet worden uitgeschakeld.
- Bij gebruik van identiteitscontrole op basis van certificaten moet de server zo zijn ingesteld dat deze de identiteit van de gebruikersgroep kan vaststellen op basis van velden in het clientcertificaat. Zie “Identiteitscontrolegroepen” op pagina 75.

IPSec-instellingen

Gebruik de volgende IPSec-instellingen:

- Mode: 'Tunnel Mode'
- IKE Exchange Modes: 'Aggressive Mode' voor hybride identiteitscontrole en controle op basis van een vooraf gedeelde sleutel, 'Main Mode' voor identiteitscontrole op basis van certificaten.
- Encryption Algorithms: 3DES, AES-128, AES-256
- Authentication Algorithms: HMAC-MD5, HMAC-SHA1
- Diffie Hellman Groups: 'Group 2' is vereist voor hybride identiteitscontrole en controle op basis van een vooraf gedeelde sleutel. Voor identiteitscontrole op basis van certificaten gebruikt u 'Group 2' met 3DES en AES-128. Gebruik 'Group 2' of 'Group 5' met AES-256.
- PFS (Perfect Forward Secrecy): Voor IKE fase 2 moet bij gebruik van PFS dezelfde Diffie-Hellman-groep worden gebruikt als voor IKE fase 1.
- Mode Configuration: Moet zijn ingeschakeld.
- Dead Peer Detection:Aanbevolen.
- Standard NAT Traversal:Wordt ondersteund en kan desgewenst worden ingeschakeld (IPSec via TCP wordt niet ondersteund).
- Load Balancing:Wordt ondersteund en kan desgewenst worden ingeschakeld.
- Re-keying of Phase 1: Wordt momenteel niet ondersteund. Het aanbevolen interval voor re-keying op de server is ongeveer één uur.
- ASA Address Mask: Zorg ervoor dat alle adrespoolmaskers van apparaten niet zijn ingesteld of zijn ingesteld op 255.255.255.255. Een voorbeeld:

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

  Wanneer u dit aanbevolen adresmasker gebruikt, worden sommige routes die door de VPN-configuratie worden verondersteld, mogelijk genegeerd. Om dit te voorkomen zorgt u ervoor dat uw routeringstabel alle benodigde routes bevat en controleert u of de subnetadressen toegankelijk zijn voordat u een en ander implementeert.

Overige ondersteunde functies

Voor de iPhone, iPod touch en iPad kunnen de volgende functies worden gebruikt:

- Application Version:Informatie over de softwareversie op de client wordt naar de server gestuurd, zodat de server verbindingen kan toestaan of weigeren op basis van de softwareversie op het apparaat.
- Banner:Als op de server een banner is geconfigureerd, wordt deze op het apparaat weergegeven. De gebruiker kan de banner vervolgens accepteren of de verbinding verbreken.

- Split Tunnel:De functie 'Split Tunnel' wordt ondersteund.
- Split DNS:De functie 'Split DNS' wordt ondersteund.
- Default Domain:De functie 'Default Domain' wordt ondersteund.

De structuur van configuratieprofielen

Deze bijlage bevat informatie over de structuur van mobileconfig-bestanden, bedoeld voor personen die zelf programma's willen ontwikkelen.

Er wordt van uitgegaan dat u bekend bent met de Apple XML DTD-structuur en de algemene structuur van eigenschappenlijsten (plists). Een algemene beschrijving van de plist-structuur van Apple vindt u op www.apple.com/DTDs/PropertyList-1.0.dtd. U begint door met iPhone-configuratieprogramma een geraamte van een bestand aan te maken, dat u vervolgens aanpast aan de hand van de informatie in deze bijlage.

In deze bijlage komen de termen 'payload' (lading) en 'profiel' voor. Een profiel is het volledige bestand waarmee een of meer instellingen op een iPhone, iPod touch of iPad worden geconfigureerd. Een payload is een afzonderlijk onderdeel van het profielbestand.

Hoofdniveau

Op hoofdniveau is het configuratiebestand een woordenboek met de volgende sleutel/waarde-paren:

Sleutel	Waarde
PayloadVersion	Getal, verplicht. De versie van het volledige configuratieprofielbestand. Dit versienummer duidt de structuur van het volledige profiel aan, niet van de afzonderlijke payloads.
PayloadUUID	Tekenreeks, verplicht. Dit is doorgaans een kunstmatig gegenereerde unieke identificatietekenreeks. De precieze inhoud van deze tekenreeks doet er niet toe, zolang deze maar uniek is. Op Mac OS X kunt u UUID's genereren met /usr/bin/uuidgen.
PayloadType	Tekenreeks, verplicht. Vooralsnog is 'Configuration' de enige geldige waarde voor deze sleutel.
PayloadOrganization	Tekenreeks, optioneel. Deze waarde geeft aan door welke organisatie het profiel is uitgegeven. Deze informatie is zichtbaar voor de gebruiker.

Sleutel	Waarde
PayloadIdentifier	Tekenreeks, verplicht. Standaard een door punten gescheiden tekenreeks die een unieke beschrijving geeft van het profiel, bijvoorbeeld 'com.mijnBedrijf.iPhone.mailinstellingen' of 'edu.mijnSchool.studenten.vpn'. Op basis van deze tekenreeks kunnen profielen van elkaar worden onderscheiden. Als een profiel wordt geïnstalleerd dat dezelfde aanduiding heeft als een ander profiel, wordt het bestaande profiel overschreven (in plaats van dat het nieuwe profiel naast het andere wordt toegevoegd).
PayloadDisplayName	Tekenreeks, verplicht. Een zeer korte tekenreeks die als beschrijving van het profiel aan de gebruiker wordt getoond, bijvoorbeeld 'VPN-instellingen'. Deze waarde hoeft niet uniek te zijn.
PayloadDescription	Tekenreeks, optioneel. Beschrijvende tekst die de gebruiker te zien krijgt in het detailscherm van het volledige profiel. De tekst moet duidelijk aangeven waartoe het profiel dient, zodat de gebruiker kan beslissen of hij of zij dit profiel wil installeren.
PayloadContent	Array, optioneel. De feitelijke inhoud van het profiel. Als deze waarde wordt weggelaten, heeft het profiel als geheel geen functionele betekenis.
PayloadRemovalDisallowed	Booleaanse waarde, optioneel. Standaard ingesteld op onwaar. Als deze sleutel is ingesteld, kan de gebruiker het profiel niet verwijderen. Profielen waarvoor deze sleutel is ingesteld, kunnen alleen via USB, het web of via e-mail worden bijgewerkt als de profielaanduiding overeenkomt en door dezelfde autoriteit is ondertekend. Als er een wachtwoord voor het verwijderen van het profiel is ingesteld, kan het profiel worden verwijderd door het wachtwoord op te geven. Als u deze coderingsbits voor ondertekende en gecodeerde profielen in de eenvoudige weergave gebruikt, heeft dit geen gevolgen omdat het profiel niet kan worden gewijzigd en deze instelling ook op het apparaat wordt weergegeven.

Inhoud van de payload

De PayloadContent-array is een array van woordenboeken, waarbij per woordenboek van elke afzonderlijke payload van het profiel een beschrijving wordt gegeven. Elk functioneel profiel heeft een PayloadContent-array met minimaal één vermelding. Alle woordenboeken in deze array hebben een aantal gemeenschappelijke eigenschappen, ongeacht het payloadtype. Daarnaast zijn er per payloadtype enkele specifieke en unieke eigenschappen.

Sleutel	Waarde
PayloadVersion	Getal, verplicht. De versie van de afzonderlijke payload. Elk profiel kan uit payloads met verschillende versienummers bestaan. De VPN-payload kan op een bepaald moment bijvoorbeeld een hoger versienummer krijgen, terwijl het versienummer van de e-mailpayload gelijk blijft.
PayloadUUID	Tekenreeks, verplicht. Dit is doorgaans een kunstmatig gegenereerde unieke identificatietekenreeks. De precieze inhoud van deze tekenreeks doet er niet toe, zolang deze maar uniek is.
PayloadType	Tekenreeks, verplicht. Dit sleutel/waarde-paar geeft voor elke afzonderlijke payload in het profiel het payloadtype aan.
PayloadOrganization	Tekenreeks, optioneel. Deze waarde geeft aan door welke organisatie het profiel is uitgegeven. Deze informatie is zichtbaar voor de gebruiker. Deze waarde kan al dan niet gelijk zijn aan die van de PayloadOrganization-sleutel op hoofdniveau.
PayloadIdentifier	Tekenreeks, verplicht. Standaard een door punten gescheiden tekenreeks die een unieke beschrijving geeft van de payload. Doorgaans is deze waarde gelijk aan de PayloadIdentifier op hoofdniveau, aangevuld met een subaanduiding voor de desbetreffende payload.
PayloadDisplayName	Tekenreeks, verplicht. Een zeer korte tekenreeks die als beschrijving van het profiel aan de gebruiker wordt getoond, bijvoorbeeld 'VPN-instellingen'. Deze waarde hoeft niet uniek te zijn.
PayloadDescription	Tekenreeks, optioneel. Beschrijvende tekst die de gebruiker te zien krijgt in het detailscherm van de desbetreffende payload.

Profile Removal Password Payload

De Removal Password-payload wordt aangeduid met de PayloadType-waarde com.apple.profileRemovalPassword. Het doel van deze payload is het wachtwoord te coderen waarmee gebruikers een configuratieprofiel van het apparaat kunnen verwijderen. Als deze payload aanwezig is en voor de payload een waarde voor het wachtwoord is opgegeven, wordt om het wachtwoord gevraagd wanneer de gebruiker op de knop 'Verwijder' in het profiel tikt. Deze payload is gecodeerd met de rest van het profiel.

Sleutel	Waarde
RemovalPassword	Tekenreeks, optioneel. Hiermee wordt het wachtwoord voor verwijderen van het profiel opgegeven.

De payload 'Toegangscode'

De payload 'Toegangscode' wordt aangeduid met de PayloadType-waarde com.apple.mobiledevice.passwordpolicy. Als dit payloadtype is ingesteld, wordt op het apparaat een mechanisme voor het invoeren van een alfanumerieke toegangscode geactiveerd, dat invoer van al dan niet lange en complexe toegangscodes mogelijk maakt.

Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
allowSimple	Booleaanse waarde, optioneel. Standaard ingesteld op waar. Hiermee wordt bepaald of een eenvoudige toegangscode is toegestaan. Een eenvoudige toegangscode is een code waarin tekens worden herhaald of in een oplopende of aflopende reeks worden gebruikt (zoals 123 of CBA). Het instellen van deze eigenschap op onwaar heeft hetzelfde effect als het instellen van minComplexChars op '1'.
forcePIN	Booleaanse waarde, optioneel. Standaard ingesteld op onwaar. Hiermee wordt bepaald of de gebruiker verplicht een pincode moet instellen. Als u alleen deze waarde en geen andere waarden instelt, moet de gebruiker een toegangscode invoeren, maar worden geen eisen gesteld aan de lengte of complexiteit.
maxFailedAttempts	Getal, optioneel. De standaardwaarde is 11. Het toegestane bereik is [2...11]. Hiermee wordt aangegeven hoe vaak mag worden geprobeerd om de juiste toegangscode in te voeren voor het ontgrendelen van het apparaat. Zodra dit aantal wordt overschreden, wordt het apparaat vergrendeld en kan het alleen worden ontgrendeld door het op de specifiek aangewezen computer met iTunes aan te sluiten.

Sleutel	Waarde
maxInactivity	Getal, optioneel. De standaardwaarde is 'Infinity'. Hiermee wordt aangegeven na hoeveel minuten inactiviteit (zonder dat de gebruiker het apparaat heeft ontgrendeld) het apparaat door het systeem wordt vergrendeld. Zodra deze limiet is bereikt, wordt het apparaat vergrendeld en moet de toegangscode worden ingevoerd.
maxPINAgeInDays	Getal, optioneel. De standaardwaarde is 'Infinity'. Hiermee wordt aangegeven hoeveel dagen de toegangscode ongewijzigd kan blijven. Als dit aantal dagen is verstreken, moet de gebruiker de toegangscode wijzigen om het apparaat te kunnen ontgrendelen.
minComplexChars	Getal, optioneel. De standaardwaarde is '0'. Hiermee wordt aangegeven hoeveel complexe tekens er minimaal in de toegangscode moeten voorkomen. Een "complex" teken is een teken dat geen cijfer of letter is, zoals &%$#.
minLength	Getal, optioneel. De standaardwaarde is '0'. Hiermee wordt aangegeven hoe lang de gehele toegangscode minimaal moet zijn. Deze eigenschap staat los van de eveneens optionele eigenschap minComplexChars.
requireAlphanumeric	Booleaanse waarde, optioneel. Standaard ingesteld op onwaar. Hiermee wordt aangegeven of de gebruiker tekens uit het alfabet moet invoeren (abcd) of dat alleen cijfers voldoende zijn.
pinHistory	Getal, optioneel. Bij het wijzigen van de toegangscode moet de gebruiker er rekening mee houden dat de code uniek moet zijn voor de laatste N-vermeldingen in de geschiedenis. De minimumwaarde is 1, de maximumwaarde is 50.
manualFetchingWhenRoaming	Booleaanse waarde, optioneel. Als deze sleutel is ingesteld, worden alle pushbewerkingen tijdens het roamen uitgeschakeld. Nieuwe gegevens moeten handmatig worden opgehaald.
maxGracePeriod	Getal, optioneel. De maximumuitstelperiode (in minuten) dat de telefoon ontgrendeld is zonder een toegangscode te hoeven invoeren. Als de standaardwaarde '0' (geen uitstelperiode) is ingesteld, moet direct een toegangscode worden ingevoerd.

De payload 'E-mail'

De payload 'E-mail' wordt aangeduid met de PayloadType-waarde com.apple.mail.managed. Met deze payload wordt een e-mailaccount op het apparaat aangemaakt. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
EmailAccountDescription	Tekenreeks, optioneel. Een beschrijving van de e-mailaccount, die de gebruiker te zien krijgt in de programma's Mail en Instellingen.
EmailAccountName	Tekenreeks, optioneel. De volledige gebruikersnaam voor de account. Deze naam is onder andere te zien in verstuurde berichten.
EmailAccountType	Tekenreeks, verplicht. Toegestane waarden zijn 'EmailTypePOP' en 'EmailTypeIMAP'. Hiermee wordt aangegeven welk protocol voor deze account moet worden gebruikt.
EmailAddress	Tekenreeks, verplicht. Het volledige e-mailadres voor de account. Als deze waarde niet in de payload is opgenomen, wordt er bij het installeren van het profiel alsnog om gevraagd.
IncomingMailServerAuthentication	Tekenreeks, verplicht. De methode voor identiteitscontrole voor inkomende post. Toegestane waarden zijn 'EmailAuthPassword' en 'EmailAuthNone'.
IncomingMailServerHostName	Tekenreeks, verplicht. De hostnaam (of het IP-adres) van de server voor inkomende post.
IncomingMailServerPortNumber	Getal, optioneel. Het poortnummer van de server voor inkomende post. Als er geen poortnummer is opgegeven, wordt de standaardpoort voor een gegeven protocol gebruikt.
IncomingMailServerUseSSL	Booleaanse waarde, optioneel. Standaard ingesteld op waar. Hiermee wordt aangegeven of op de server voor inkomende post identiteitscontrole via SSL wordt toegepast.
IncomingMailServerUsername	Tekenreeks, verplicht. De gebruikersnaam voor de e-mailaccount, doorgaans gelijk aan het e-mailadres tot aan het @-teken. Als deze waarde niet in de payload is opgenomen en als voor de account identiteitscontrole voor inkomende post is ingesteld, wordt bij het installeren van het profiel om deze waarde gevraagd.
IncomingPassword	Tekenreeks, optioneel. Het wachtwoord voor de server voor inkomende post. Gebruik deze sleutel alleen in combinatie met gecodeerde profielen.
OutgoingPassword	Tekenreeks, optioneel. Het wachtwoord voor de server voor uitgaande post. Gebruik deze sleutel alleen in combinatie met gecodeerde profielen.
OutgoingPasswwordSameAsIncomingPassword	Booleaanse waarde, optioneel. Als deze sleutel is ingesteld, wordt de gebruiker slechts eenmaal gevraagd het wachtwoord in te voeren, waarna het wachtwoord wordt gebruikt voor zowel uitgaande als inkomende post.

Sleutel	Waarde
OutgoingMailServerAuthentication	Tekenreeks, verplicht. De methode voor identiteitscontrole voor uitgaande post. Toegestane waarden zijn 'EmailAuthPassword' en 'EmailAuthNone'.
OutgoingMailServerHostName	Tekenreeks, verplicht. De hostnaam (of het IP-adres) van de server voor uitgaande post.
OutgoingMailServerPortNumber	Getal, optioneel. Het poortnummer van de server voor uitgaande post. Als er geen poortnummer is opgegeven, wordt poort 25, 587 of 465 gebruikt (het eerstgenoemde nummer eerst).
OutgoingMailServerUseSSL	Booleaanse waarde, optioneel. Standaard ingesteld op waar. Hiermee wordt aangegeven of op de server voor uitgaande post identiteitscontrole via SSL wordt toegepast.
OutgoingMailServerUsername	Tekenreeks, verplicht. De gebruikersnaam voor de e-mailaccount, doorgaans gelijk aan het e-mailadres tot aan het @-teken. Als deze waarde niet in de payload is opgenomen en als voor de account identiteitscontrole voor uitgaande post is ingesteld, wordt bij het installeren van het profiel om deze waarde gevraagd.

De payload 'Webknipsels'

De payload 'Webknipsels' wordt aangeduid met de PayloadType-waarde com.apple.webClip.managed. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
URL	Tekenreeks, verplicht. De URL die wordt geopend wanneer op het webknipsel wordt geklikt. De URL moet beginnen met HTTP of HTTPS. Als dit niet het geval is, werkt de URL niet.
Label	Tekenreeks, verplicht. De naam van het webknipsel zoals in het beginscherm wordt weergegeven.
Icon	Gegevens, optioneel. Een PNG-symbool dat in het beginscherm wordt weergegeven. De afmeting van het symbool moet 59 x 60 pixels zijn. Als u geen symbool opgeeft, wordt een wit vierkant weergegeven.
IsRemovable	Booleaanse waarde, optioneel. Als deze waarde is ingesteld op onwaar, kan de gebruiker het webknipsel niet verwijderen, maar wordt het webknipsel verwijderd zodra het profiel wordt verwijderd.

De payload 'Beperkingen'

De payload 'Beperkingen' wordt aangeduid met de PayloadType-waarde com.apple.applicationaccess. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
allowAppInstallation	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt de App Store uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Gebruikers kunnen geen programma's installeren of bijwerken.
allowCamera	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt de camera volledig uitgeschakeld en wordt het camerasymbool uit het beginscherm verwijderd. Gebruikers kunnen geen foto's maken.
allowExplicitContent	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt expliciet muziek- of videomateriaal dat via de iTunes Store is aangeschaft, verborgen. Expliciet materiaal wordt als zodanig aangeduid door de aanbieders van het materiaal (zoals platenlabels) bij de verkoop via de iTunes Store.
allowScreenShot	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, kunnen gebruikers geen schermafbeelding bewaren.
allowYouTube	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt het programma YouTube uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd.
allowiTunes	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt de iTunes Store uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Gebruikers kunnen materiaal niet vooraf bekijken of beluisteren en geen materiaal aanschaffen of downloaden.
allowSafari	Booleaanse waarde, optioneel. Wanneer deze eigenschap onwaar is, wordt het programma Safari uitgeschakeld en wordt het programmasymbool uit het beginscherm verwijderd. Met deze optie kunt u ook voorkomen dat gebruikers webknipsels kunnen openen.

De payload 'LDAP'

De payload 'LDAP' wordt aangeduid met de PayloadType-waarde com.apple.ldap.account. Er bestaat een één-op-veel relatie tussen de LDAP-account en LDAPSearchSettings. LDAP is vergelijkbaar met een boomstructuur. Elk SearchSettings-object vertegenwoordigt een node in de hiërarchie dat fungeert als startpunt voor zoekacties, en het bereik waarin moet worden gezocht (node, node + 1 niveau met onderliggende onderdelen, node + alle niveaus met onderliggende onderdelen). Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
LDAPAccountDescription	Tekenreeks, optioneel. Beschrijving van de account.
LDAPAccountHostName	Tekenreeks, verplicht. De host.
LDAPAccountUseSSL	Booleaanse waarde, verplicht. Hiermee wordt aangegeven of gebruik moet worden gemaakt van SSL.
LDAPAccountUserName	Tekenreeks, optioneel. De gebruikersnaam.
LDAPAccountPassword	Tekenreeks, optioneel. Gebruik deze sleutel alleen in combinatie met gecodeerde profielen.
LDAPSearchSettings	Containerobject op het hoogste niveau. Voor een account kunnen meerdere exemplaren van deze sleutel aanwezig zijn. Deze sleutel is alleen nuttig als voor de account minimaal één exemplaar van de sleutel is ingesteld.
LDAPSearchSettingDescription	Tekenreeks, optioneel. De beschrijving van deze zoekinstelling.
LDAPSearchSettingSearchBase	Tekenreeks, vereist. Conceptueel gezien is dit het pad naar de node dat het startpunt vormt voor een zoekactie ('ou=people,o=example corp').
LDAPSearchSettingScope	Tekenreeks, vereist. Hiermee wordt gedefinieerd welke recursie in de zoekactie moet worden gebruikt. U kunt een van de volgende drie waarden gebruiken: LDAPSearchSettingScopeBase: Alleen de directe node waarnaar SearchBase verwijst. LDAPSearchSettingScopeOneLevel: De node plus de directe onderliggende onderdelen. LDAPSearchSettingScopeSubtree: De node plus alle onderliggende onderdelen, ongeacht de diepte.

De payload 'CalDAV'

De payload 'CalDAV' wordt aangeduid met de PayloadType-waarde com.apple.caldav.account. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
CalDAVAccountDescription	Tekenreeks, optioneel. Beschrijving van de account.
CalDAVHostName	Tekenreeks, verplicht. Het serveradres.
CalDAVUsername	Tekenreeks, verplicht. De inlognaam van de gebruiker.
CalDAVPassword	Tekenreeks, optioneel. Het wachtwoord van de gebruiker.
CalDAVUseSSL	Booleaanse waarde, verplicht. Hiermee wordt aangegeven of gebruik moet worden gemaakt van SSL.
CalDAVPort	Getal, optioneel. De poort waarmee verbinding met de server wordt gemaakt.
CalDAVPrincipalURL	Tekenreeks, optioneel. De basis-URL naar de agenda van de gebruiker.

De payload 'Agenda's met abonnement'

De payload 'Agenda's met abonnement' wordt aangeduid met de PayloadType-waarde com.apple.subscribedcalendar.account. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
SubCalAccountDescription	Tekenreeks, optioneel. Beschrijving van de account.
SubCalAccountHostName	Tekenreeks, verplicht. Het serveradres.
SubCalAccountUsername	Tekenreeks, optioneel. De inlognaam van de gebruiker.
SubCalAccountPassword	Tekenreeks, optioneel. Het wachtwoord van de gebruiker.
SubCalAccountUseSSL	Booleaanse waarde, verplicht. Hiermee wordt aangegeven of gebruik moet worden gemaakt van SSL.

De payload 'SCEP'

De payload 'SCEP' (Simple Certificate Enrollment Protocol) wordt aangeduid met de PayloadType-waarde com.apple.encrypted-profile-service. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
URL	Tekenreeks, verplicht.
Naam	Tekenreeks, optioneel. Elke tekenreeks die door de SCEP-server kan worden geïnterpreteerd. Voorbeeld van een tekenreeks is een domeinnaam, zoals 'voorbeeld.org'. Als voor een certificaatautoriteit meerdere CA-certificaten aanwezig zijn, kunt u in dit veld aangeven welke certificaten zijn vereist.
Onderwerp	Array, optioneel. De weergave van een X.500-naam, aangeduid als een array bestaande uit een object-ID en een waarde. Bijvoorbeeld: '/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar', wat het volgende inhoudt: [[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]] Object-ID's kunnen worden weergegeven als getallen met punten, met snelkoppelingen voor C, L, ST, O, OU, CN (land, plaats, provincie, organisatie, organisatie-eenheid, algemene naam).
Challenge	Tekenreeks, optioneel. Een vooraf gedeeld geheim.
Keysize	Getal, optioneel. De sleutelgrootte in bits (1024 of 2048).
Key Type	Tekenreeks, optioneel. Momenteel altijd 'RSA'.
Key Usage	Getal, optioneel. Een bitmasker waarmee het gebruik van de sleutel wordt aangegeven. 1 staat voor ondertekenen, 4 voor coderen en 5 voor zowel ondertekenen als coderen. Sommige CA's, zoals de Windows-CA, ondersteunen alleen codering of ondertekening, maar niet beide tegelijkertijd.

SubjectAltName-woordenboeksleutels

Met de payload 'SCEP' kunt u een optioneel SubjectAltName-woordenboek opgeven dat waarden aanlevert die de CA nodig heeft om een certificaat uit te geven. Voor elke sleutel kunt u één tekenreeks of een array met tekenreeksen opgeven. De waarden die u opgeeft, hangen af van de CA die u gebruikt, maar kunnen een DNS-naam, een URL of e-mailwaarden zijn. Zie “Fase 3: Serverrespons met SCEP-specificaties - voorbeeld” op pagina 96 voor een voorbeeld.

GetCACaps-woordenboeksleutels

Als u een woordenboek met de sleutel 'GetCACaps' toevoegt, worden de tekenreeksen die u opgeeft door het apparaat beschouwd als gezaghebbende bron van informatie over de mogelijkheden van uw CA. In andere gevallen vraagt het apparaat de CA om GetCACaps en gebruikt het apparaat het antwoord dat het daarop krijgt. Als de CA niet reageert, gebruikt het apparaat standaard de GET 3DES- en SHA-1-aanvragen.

De payload 'APN'

De payload 'APN' (Access Point Name, naam toegangspunt) wordt aangeduid met de PayloadType-waarde com.apple.apn.managed. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
DefaultsData	Woordenboek, verplicht. Dit woordenboek bevat twee sleutel/waarde-paren.
DefaultsDomainName	Tekenreeks, verplicht. De enige toegestane waarde is 'com.apple.managedCarrier'.
apns	Array, verplicht. Deze array bevat een willekeurig aantal woordenboeken, één woordenboek voor elke APN-configuratie, met de volgende sleutel/waarde-paren.
apn	Tekenreeks, verplicht. Hiermee wordt de naam van het toegangspunt opgegeven.
username	Tekenreeks, verplicht. Hiermee wordt de gebruikersnaam voor dit toegangspunt opgegeven. Als deze waarde ontbreekt, wordt er bij het installeren van het profiel alsnog om gevraagd.
password	Gegevens, optioneel. Het wachtwoord dat de gebruiker nodig heeft voor dit toegangspunt. Om veiligheidsredenen wordt het wachtwoord onleesbaar gemaakt. Als deze waarde ontbreekt in de payload, wordt er bij het installeren van het profiel alsnog om gevraagd.
proxy	Tekenreeks, optioneel. Het IP-adres of de URL van de APN-proxy.
proxyPort	Getal, optioneel. Het poortnummer van de APN-proxy.

De payload 'Exchange'

De payload 'Exchange' wordt aangeduid met de PayloadType-waarde com.apple.eas.account. Met deze payload wordt een Microsoft Exchange-account op het apparaat aangemaakt. Naast de eigenschappen die op alle payloads van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen:

Sleutel	Waarde
EmailAddress	Tekenreeks, verplicht. Als deze waarde niet in de payload is opgenomen, wordt er bij het installeren van het profiel alsnog om gevraagd. Hiermee wordt het volledige e-mailadres voor de account opgegeven.
Host	Tekenreeks, verplicht. De hostnaam (of het IP-adres) van de Exchange-server.
SSL	Booleaanse waarde, optioneel. Standaard ingesteld op waar. Hiermee wordt aangegeven of op de Exchange-server identiteitscontrole via SSL wordt toegepast.

Sleutel	Waarde
UserName	Tekenreeks, verplicht. De gebruikersnaam voor deze Exchange-account. Als deze waarde ontbreekt, wordt er bij het installeren van het profiel alsnog om gevraagd.
Wachtwoord	Tekenreeks, optioneel. Het wachtwoord van de account. Gebruik deze sleutel alleen in combinatie met gecodeerde profielen.
Certificate	Optioneel. Voor accounts die met een certificaat kunnen worden geverifieerd, is dit een .p12-identiteitscertificaat in de NSData-blobstructuur.
CertificateName	Tekenreeks, optioneel. Geeft de naam of beschrijving van het certificaat aan.
CertificatePassword	Optioneel. Het wachtwoord dat nodig is voor het .p12-identiteitscertificaat. Gebruik deze sleutel alleen in combinatie met gecodeerde profielen.

De payload 'VPN'

De payload 'VPN' wordt aangeduid met de PayloadType-waarde com.apple.vpn.managed. Naast de eigenschappen die op alle payloadtypen van toepassing zijn, heeft de VPN-payload de volgende specifieke eigenschappen.

Sleutel	Waarde
UserDefinedName	Tekenreeks. Beschrijving van de VPN-verbinding die op het apparaat wordt weergegeven.
OverridePrimary	Booleaanse waarde. Hiermee wordt aangegeven of al het verkeer via de VPN-interface moet lopen. Als deze eigenschap op waar is ingesteld, loopt al het netwerkverkeer via VPN.
VPNType	Tekenreeks. Hiermee wordt bepaald welke instellingen beschikbaar zijn in de payload, afhankelijk van het type VPN-verbinding. Er zijn drie mogelijke waarden: 'L2TP', 'PPTP' of 'IPSec', aanduidingen voor respectievelijk L2TP, PPTP en Cisco IPSec.

Op het hoogste niveau kunnen twee woordenboeken zijn opgenomen, onder de sleutels 'PPP' en 'IPSec'. De sleutels in deze twee woordenboeken worden hierna beschreven. Ook wordt aangegeven onder welke VPNType-waarde de sleutels worden gebruikt.

PPP-woordenboeksleutels

De volgende elementen worden gebruikt voor VPN-payloads van het type 'PPP'.

Sleutel	Waarde
AuthName	Tekenreeks. De gebruikersnaam voor de VPN-account. Gebruikt voor L2TP en PPTP.
AuthPassword	Tekenreeks, optioneel. Alleen zichtbaar als TokenCard op onwaar is ingesteld. Gebruikt voor L2TP en PPTP.
TokenCard	Booleaanse waarde. Hiermee wordt aangegeven of voor het maken van een verbinding een tokenkaart, zoals een RSA SecurID-kaart, moet worden gebruikt. Gebruikt voor L2TP.
CommRemoteAddress	Tekenreeks. Het IP-adres of de hostnaam van de VPN-server. Gebruikt voor L2TP en PPTP.
AuthEAPPlugins	Array. Deze sleutel komt alleen voor als RSA SecurID wordt gebruikt en heeft in dat geval één vermelding: een tekenreeks met de waarde 'EAP-RSA'. Gebruikt voor L2TP en PPTP.
AuthProtocol	Array. Deze sleutel komt alleen voor als RSA SecurID wordt gebruikt en heeft in dat geval één vermelding: een tekenreeks met de waarde 'EAP'. Gebruikt voor L2TP en PPTP.
CCPMPPE40Enabled	Booleaanse waarde. Zie de uitleg bij 'CCPEnabled'. Gebruikt voor PPTP.
CCPMPPE128Enabled	Booleaanse waarde. Zie de uitleg bij 'CCPEnabled'. Gebruikt voor PPTP.
CCPEnabled	Booleaanse waarde. Hiermee wordt codering ingeschakeld voor de verbinding. Als deze sleutel en 'CCPMPPE40Enabled' op waar zijn ingesteld, wordt het coderingsniveau automatisch vastgesteld. Als deze sleutel en 'CCPMPPE128Enabled' op waar zijn ingesteld, wordt het maximale coderingsniveau toegepast. Als geen codering wordt toegepast, is geen enkele CCP-sleutel op waar ingesteld. Gebruikt voor PPTP.

IPsec-woordenboeksleutels

De volgende elementen worden gebruikt voor VPN-payloads van het type 'IPsec'.

Sleutel	Waarde
RemoteAddress	Tekenreeks. Het IP-adres of de hostnaam van de VPN-server. Gebruikt voor Cisco IPSec.
AuthenticationMethod	Tekenreeks. 'SharedSecret' of 'Certificate'. Gebruikt voor L2TP en Cisco IPSec.
XAuthName	Tekenreeks. De gebruikersnaam voor de VPN-account. Gebruikt voor Cisco IPSec.
XAuthEnabled	Geheel getal. 1 als XAUTH is ingeschakeld en 0 indien uitgeschakeld. Gebruikt voor Cisco IPSec.

Sleutel	Waarde
LocalIdentifier	Tekenreeks. Wordt alleen gebruikt als AuthenticationMethod = SharedSecret. De naam van de te gebruiken groep. Als hybride identiteitscontrole wordt gebruikt, moet de tekenreeks eindigen op '[hybrid]'. Gebruikt voor Cisco IPSec.
LocalIdentifierType	Tekenreeks. Wordt alleen gebruikt als AuthenticationMethod = SharedSecret. De waarde is 'KeyID'. Gebruikt voor L2TP en Cisco IPSec.
SharedSecret	Gegevens. Het gedeelde geheim voor deze VPN-account. Wordt alleen gebruikt als AuthenticationMethod = SharedSecret. Gebruikt voor L2TP en Cisco IPSec.
PayloadCertificateUUID	Tekenreeks. De UUID van het certificaat dat voor de legitimatie van de account moet worden gebruikt. Wordt alleen gebruikt als AuthenticationMethod = Certificate. Gebruikt voor Cisco IPSec.
PromptForVPNPIN	Booleaanse waarde. Hiermee wordt aangegeven of bij het maken van een verbinding om een pincode moet worden gevraagd. Gebruikt voor Cisco IPSec.

De payload 'Wi-Fi'

De payload 'Wi-Fi' wordt aangeduid met de PayloadType-waarde com.apple.wifi.managed. Hiermee wordt versie 0 van de PayloadVersion-waarde beschreven. Naast de eigenschappen die op alle payloadtypen van toepassing zijn, heeft deze payload de volgende specifieke eigenschappen.

Sleutel	Waarde
SSID_STR	Tekenreeks. De SSID van het te gebruiken Wi-Fi-netwerk.
HIDDEN_NETWORK	Booleaanse waarde. Naast de SSID worden gegevens als het uitzend- en coderingstype gebruikt om onderscheid tussen netwerken te maken. Standaard wordt ervan uitgegaan dat alle geconfigureerde netwerken open zijn of uitzenden. Om een verborgen netwerk op te geven, moet u een booleaanse waarde instellen voor de sleutel 'HIDDEN_NETWORK'.
EncryptionType	Tekenreeks. De mogelijke waarden voor 'EncryptionType' zijn 'WEP', 'WPA' en 'Any'. 'WPA' staat voor WPA en WPA2 en is op beide coderingstypen van toepassing. Zorg ervoor dat de waarde die u instelt, overeenkomt met de mogelijkheden van het netwerktoegangspunt. Als u niet weet welk coderingstype u moet instellen of als u wilt dat alle coderingstypen mogelijk zijn, stelt u de waarde 'Any' in.
Wachtwoord	Tekenreeks, optioneel. Ook als u geen wachtwoord voor het netwerk opgeeft, wordt het netwerk aan de lijst met bekende netwerken toegevoegd. Zodra de gebruiker verbinding met dat netwerk probeert te maken, wordt alsnog om een wachtwoord gevraagd.

Voor 802.1X-bedrijfsnetwerken moet het EAPClientConfiguration-woordenboek worden opgegeven.

EAPClientConfiguration-woordenboek

Naast de standaardcoderingstypen is het mogelijk om voor een bepaald netwerk een bedrijfsprofiel op te geven door middel van de sleutel 'EAPClientConfiguration'. Als de sleutel wordt opgegeven, moet als waarde een woordenboek met de volgende sleutels worden gebruikt.

Sleutel	Waarde
UserName	Tekenreeks, optioneel. Deze eigenschap komt alleen in een geïmporteerde configuratie voor als de exacte gebruikersnaam bekend is. Gebruikers kunnen deze informatie invoeren tijdens de identiteitscontrole.
AcceptEAPTypes	Array met gehele getallen. De volgende EAP-typen worden geaccepteerd: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
PayloadCertificateAnchorUUID	Array met tekenreeksen, optioneel. Hiermee worden de certificaten geïdentificeerd die voor deze identiteitscontrole moeten worden vertrouwd. Elke invoer moet de UUID van de certificaatpayload bevatten. Met deze sleutel voorkomt u dat een gebruiker wordt gevraagd of de genoemde certificaten kunnen worden vertrouwd. Als deze eigenschap wordt opgegeven, wordt het dynamisch instellen van vertrouwen (via het certificaatvenster) uitgeschakeld. Dit geldt echter niet als 'TLSAllowTrustExceptions' op waar wordt ingesteld.
TLSTrustedServerNames	Array met tekenreekswaarden, optioneel. Dit is de lijst met geaccepteerde algemene namen voor servercertificaten. U kunt voor de naam gebruikmaken van jokertekens, bijvoorbeeld wpa.*.voorbeeld.com. Als een server een certificaat toont dat niet in deze lijst voorkomt, wordt het certificaat niet vertrouwd. Met deze eigenschap, alleen of in combinatie met 'TLSTrustedCertificates', kan iemand precies aangeven welke certificaten voor het opgegeven netwerk moeten worden vertrouwd en zo voorkomen dat certificaten dynamisch moeten worden vertrouwd. Als deze eigenschap wordt opgegeven, wordt het dynamisch instellen van vertrouwen (via het certificaatvenster) uitgeschakeld. Dit geldt echter niet als 'TLSAllowTrustExceptions' op waar wordt ingesteld.

Sleutel	Waarde
TLSAllowTrustExceptions	Booleaanse waarde, optioneel. Hiermee wordt bepaald of de gebruiker dynamisch vertrouwen mag instellen. Vertrouwen wordt dynamisch ingesteld in het certificaatvenster dat verschijnt wanneer een certificaat niet wordt vertrouwd. Als deze eigenschap op onwaar is ingesteld, wordt de identiteit niet geaccepteerd als het certificaat nog niet wordt vertrouwd. Zie 'PayloadCertificateAnchorUUID' en 'TLSTrustedNames' hiervoor. Deze eigenschap is standaard op waar ingesteld, behalve als 'PayloadCertificateAnchorUUID' of 'TLSTrustedServerNames' is opgegeven. In dat geval is de standaardwaarde onwaar.
TTLSInnerAuthentication	Tekenreeks, optioneel. Dit is de interne identiteitscontrole die door de TTLS-module wordt gebruikt. De standaardwaarde is 'MSCHAPv2'. Mogelijke waarden zijn 'PAP', 'CHAP', 'MSCHAP' en 'MSCHAPv2'.
OuterIdentity	Tekenreeks, optioneel. Deze sleutel is alleen relevant voor TTLS, PEAP en EAP-FAST. Hiermee kan de gebruiker zijn of haar identiteit verbergen. De werkelijke naam van de gebruiker verschijnt alleen binnen de gecodeerde tunnel. Als waarde kan bijvoorbeeld 'anoniem' of 'anon' worden ingesteld, of 'anon@mijnbedrijf.net'. Op deze manier kan de beveiliging worden verbeterd, omdat de naam van de inloggende gebruiker niet voor iedereen zichtbaar is.

Ondersteuning voor EAP-FAST

De EAP-FAST-module gebruikt de volgende eigenschappen in het EAPClientConfiguration-woordenboek.

Sleutel	Waarde
EAPFASTUsePAC	Booleaanse waarde, optioneel.
EAPFASTProvisionPAC	Booleaanse waarde, optioneel.
EAPFASTProvisionPACAnonymously	Booleaanse waarde, optioneel.

Deze sleutels worden in hiërarchische volgorde toegepast:Als 'EAPFASTUsePAC' onwaar is, worden de andere twee eigenschappen niet gebruikt. Als 'EAPFASTProvisionPAC' onwaar is, wordt de eigenschap 'EAPFASTProvisionPACAnonymously' niet gebruikt.

Als 'EAPFASTUsePAC' onwaar is, verloopt de identiteitscontrole op vrijwel dezelfde manier als bij PEAP of TTLS: De server gebruikt steeds een certificaat als bewijs van de identiteit.

Als 'EAPFASTUsePAC' waar is, wordt een bestaand PAC-bestand gebruikt, indien aanwezig. Vooralsnog kan een PAC-bestand alleen aan het apparaat worden toegevoegd als de verschaffing van PAC's is toegestaan. Hiervoor moet u 'EAPFASTProvisionPAC' inschakelen en desgewenst 'EAPFASTProvisionPACAnonymously'. 'EAPFASTProvisionPACAnonymously' is minder veilig: De identiteit van de server wordt niet gecontroleerd, zodat verbindingen kwetsbaar zijn voor man-in-the-middle-aanvallen.

Certificaten

Net als bij een VPN-configuratie is het mogelijk om de configuratie van een certificaatidentiteit aan een Wi-Fi-configuratie te koppelen. Dit is handig wanneer u legitimatiegegevens definieert voor een beveiligd bedrijfsnetwerk. Om een identiteit te koppelen, geeft u de bijbehorende payload-UUID op met de sleutel 'PayloadCertificateUUID'.

Sleutel	Waarde
PayloadCertificateUUID	Tekenreeks. De UUID van de certificaatpayload die voor de legitimatie van de identiteit moet worden gebruikt.

Voorbeeldconfiguratieprofielen

In dit gedeelte vindt u voorbeeldprofielen die de over-the-air-aanmeldingen en -configuratie toelichten. Dit zijn slechts fragmenten en uw behoeften zullen afwijken van de voorbeelden. Zie de bijzonderheden eerder in deze bijlage voor hulp bij de syntaxis. Zie “Over-the-air-aanmeldingen en -configuratie” op pagina 24 voor een beschrijving van de verschillende fasen.

Fase 1: Serverrespons - voorbeeld

```
<?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>
     or
     <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>
```

Fase 2: Apparaatrespons - voorbeeld

```
<?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>
or:
    <string>String</string>
or:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

Fase 3: Serverrespons met SCEP-specificaties - voorbeeld

```
<?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>
```

Fase 4: Apparaatrespons - voorbeeld

```
<?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>
```

Voorbeeldscripts

In deze bijlage vindt u voorbeeldscripts voor iPhone OS-implementatietaken.

De scripts in dit gedeelte moeten worden aangepast aan uw behoeften en configuraties.

Voorbeeld van C#-script voor iPhone-configuratieprogramma

Dit voorbeeldscript geeft aan hoe u configuratiebestanden aanmaakt met iPhone-configuratieprogramma voor 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.ConfigurationProfiles.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.AddRestrictionsPayload();
    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";

    }
}
```

Voorbeeld van AppleScript voor iPhone-configuratieprogramma

Dit voorbeeldscript geeft aan hoe u configuratiebestanden aanmaakt met iPhone-configuratieprogramma voor Mac OS X.

```
tell application "iPhone Configuration Utility"
  log (count of every configuration profile)
  set theProfile to make new configuration profile with properties
     {displayed name:"Profile Via Script", profile
     identifier:"com.example.configviascript", organization:"Example Org.",
     account description:"This is a configuration profile created via
     AppleScript"}
  tell theProfile
     make new passcode payload with properties {passcode required:true,
     simple 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
     Connection"}
     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
```