iPhone OS
Guide de déploiement en entreprise

Deuxième édition, pour la version 3.2 ou ultérieure

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

Publié simultanément aux États-Unis et au Canada.

F019-1835/2010-04

Table des matières

iPhone dans l'entreprise

Découvrez comment intégrer l'iPhone, l'iPod touch et l'iPad dans les systèmes de votre entreprise.

Le présent guide est destiné aux administrateurs système. Il contient des informations sur le déploiement et la prise en charge de l'iPhone, de l'iPod touch et de l'iPad dans les environnements d'entreprise.

Nouveautés d'iPhone OS 3.0 (et ultérieur) pour l'entreprise

iPhone OS 3.x comprend de nombreuses améliorations, notamment les points suivants présentant un intérêt particulier pour les utilisateurs en entreprise.

- La synchronisation sans fil de calendriers CalDAV est prise en charge.
- La prise en charge des serveurs LDAP pour la recherche de contacts dans les courriers électroniques, les carnets d'adresses et les SMS vient enrichir le logiciel.
- Les profils de configuration peuvent être chiffrés et verrouillés à un appareil donné de façon que leur suppression requière un mot de passe administrateur.
- « Utilitaire de configuration iPhone » vous permet d'ajouter et de supprimer des profils de configuration chiffrés directement sur les appareils branchés sur votre ordinateur via un câble USB.
- Le protocole OCSP (Online Certificate Status Protocol) est pris en charge pour la révocation de certificats.
- Les connexions VPN s'appuyant sur des certificats sont maintenant possibles.
- La configuration de proxy VPN par le biais d'un profil de configuration et de serveurs VPN est prise en charge.
- Les utilisateurs de Microsoft Exchange peuvent inviter d'autres utilisateurs à des réunions. Les utilisateurs de Microsoft Exchange 2007 peuvent également visualiser l'état de réponses.
- L'authentification client Exchange ActiveSync par certificat est prise en charge.
- De plus amples règlements EAS sont pris en charge, ainsi que le protocole EAS 12.1.

- D'autres restrictions sur les appareils sont disponibles, y compris la capacité de spécifier la durée pendant laquelle un appareil peut être laissé non verrouillé, de désactiver l'appareil photo et d'empêcher les utilisateurs de prendre des captures d'écran de l'appareil.
- Les messages électroniques et les événements de calendrier en local peuvent faire l'objet de recherches. En cas d'usage d'IMAP, de MobileMe et d'Exchange 2007, le courrier électronique résidant sur le serveur peut également faire l'objet de recherches.
- D'autres dossiers de courriers électroniques sont éligibles à la livraison push de courrier.
- Il est possible de préciser les réglages de proxy de service APN par le biais d'un profil de configuration.
- Les clips web sont installables à travers un profil de configuration.
- La norme 802.1x EAP-SIM est désormais prise en charge.
- Un serveur SCEP (Simple Certificate Enrollment Protocol) peut authentifier et inscrire des appareils en mode OTA.
- iTunes est en mesure de stocker des copies de sauvegarde d'appareils sous un format chiffré.
- « Utilitaire de configuration iPhone » prend en charge la création de profils via la création de scripts.
- L'Utilitaire de configuration iPhone 2.2 prend en charge l'iPad, l'iPhone et l'iPod touch. Mac OS X v10.6 Snow Leopard est requis. Windows 7 est également pris en charge.

Configuration requise

Lisez cette section si vous souhaitez obtenir une vue d'ensemble de la configuration requise et des différents composants disponibles pour l'intégration de l'iPhone, de l'iPod touch et de l'iPad dans les systèmes de votre entreprise.

iPhone et iPod touch

Les appareils iPhone et iPod touch que vous utilisez avec le réseau de votre entreprise doivent être mis à jour avec le logiciel iPhone OS 3.1.x.

iPad

L'iPad doit être mis à jour avec la version iPhone OS 3.2.x.

iTunes

iTunes 9.1 ou une version ultérieure est requis pour configurer un appareil. iTunes est également requis pour installer les mises à jour de logiciels pour l'iPhone, l'iPod touch et l'iPad. Utilisez également iTunes pour installer des applications et synchroniser de la musique, des vidéos, des notes et d'autres données avec un Mac ou un PC.

Pour utiliser iTunes, vous devez disposer d'un Mac ou d'un PC équipé d'un port USB 2.0 qui répond à la configuration minimale requise répertoriée sur le site web d'iTunes. Consultez www.apple.com/fr/itunes/download/.

« Utilitaire de configuration iPhone »

« Utilitaire de configuration iPhone » vous permet, en toute simplicité, de créer, chiffrer et installer des profils de configuration, de contrôler et installer des profils d'approvisionnement et des applications autorisées, ainsi que de capturer des renseignements sur les appareils de capture, notamment leurs historiques de console.

« Utilitaire de configuration iPhone » requiert l'un des éléments suivants :

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

« Utilitaire de configuration iPhone » fonctionne en mode 32 bits sur les versions 64 bits de Windows.

Vous pouvez télécharger le programme d'installation de .Net Framework 3.5 Service Pack 1 à l'adresse suivante : http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

L'utilitaire vous permet de créer un message Outlook avec un profil de configuration en pièce jointe. De plus, vous avez la possibilité d'attribuer des noms d'utilisateurs et des adresses électroniques issus du carnet d'adresses sur votre ordinateur de bureau à des appareils que vous avez connectés à l'utilitaire. Ces deux fonctionnalités nécessitent Outlook et sont incompatibles avec Outlook Express. Pour tirer parti de ces fonctionnalités sur des ordinateurs Windows XP, il se peut que vous deviez installer la mise à jour de « 2007 Microsoft Office System Update: Redistributable Primary Interop Assemblies ». Cette mise à jour s'avère nécessaire si Outlook est installé avant .NET Framework 3.5 Service Pack 1.

Le programme d'installation de Primary Interop Assemblies est disponible à l'adresse suivante :http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

L'iPhone, l'iPod touch et l'iPad prennent en charge les versions suivantes de Microsoft Exchange :

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

Pour la prise en charge des stratégies et des fonctionnalités d'Exchange 2007, Service Pack 1 est obligatoire.

Règlements Exchange ActiveSync pris en charge

Les stratégies Exchange suivantes sont prises en charge :

- Exiger le mot de passe sur l'appareil
- Longueur de mot de passe minimum
- Nombre maximum de tentatives de mot de passe
- Exiger tant des chiffres que des lettres
- Temps d'inactivité en minutes

Les stratégies Exchange 2007 suivantes sont en outre prises en charge :

- Autoriser ou interdire un mot de passe simple
- Expiration de mot de passe
- Historique de mot de passe
- Intervalle d'actualisation de stratégie
- Nombre minimal de caractères complexes dans les mots de passe
- Nécessiter la synchronisation manuelle lors de l'itinérance
- Autoriser l'usage de l'appareil photo
- Exige le chiffrement de l'appareil

Pour une description de chacune des stratégies, consultez la documentation fournie avec Exchange ActiveSync.

La stratégie Exchange d'exiger le chiffrement de l'appareil (RequireDeviceEncryption) est prise en charge sur l'iPhone 3GS, sur l'iPod touch (modèles 32 Go ou plus, sortis à l'automne 2009) et sur l'iPad. L'iPhone, l'iPhone 3G et les autres modèles iPod touch ne prennent pas en charge le chiffrement de l'appareil et ne peuvent pas se connecter à un serveur Exchange qui requière cette fonction.

Si vous activez le règlement « Exiger tant des chiffres que des lettres » sur Exchange 2003 ou « Exiger des valeurs alphanumériques » sur Exchange 2007, l'utilisateur devra saisir un code pour l'appareil contenant au moins un caractère complexe.

La valeur spécifiée par le règlement de délai d'inactivité (MaxInactivityTimeDeviceLock ou AEFrequencyValue) est utilisée pour définir la valeur maximale que les utilisateurs peuvent sélectionner dans Réglages > Général > Verrouillage auto. et dans Réglages > Général > Verrouillage par code > Exiger le code.

Réinitialisation à distance

Vous pouvez réinitialiser un iPhone, un iPod touch ou un iPad à distance. La réinitialisation permet de supprimer toutes les données et les informations de configuration de l'appareil. Le contenu de l'appareil est alors totalement effacé et les réglages d'origine sont restaurés.

Important : Sur l'iPhone et l'iPhone 3G, cette réinitialisation peut prendre approximativement une heure pour 8 Go d'espace disque. Branchez l'appareil à l'alimentation avant de le réinitialiser. Si l'appareil s'éteint car sa batterie se vide trop, le processus de réinitialisation reprend dès qu'il est connecté à une source d'alimentation. Sur l'iPhone 3GS et sur l'iPad, la réinitialisation supprime la clé de chiffrement des données (chiffrées en AES 256 bits) et s'exécute instantanément.

Avec Exchange Server 2007, vous pouvez lancer une réinitialisation à distance à l'aide de la console de gestion Exchange, d'Outlook Web Access ou de l'outil Exchange ActiveSync Mobile Administration Web Tool.

Avec Exchange Server 2003, vous pouvez lancer une réinitialisation à distance à l'aide de l'outil Exchange ActiveSync Mobile Administration Web Tool.

Les utilisateurs peuvent également réinitialiser un de leurs appareils en choisissant « Effacer contenu et réglages » dans le menu Réinitialiser des Réglages généraux. Vous pouvez également configurer les appareils pour qu'ils lancent immédiatement une réinitialisation après plusieurs tentatives échouées de mot de passe.

Si vous récupérez un appareil qui a été réinitialisé parce que vous l'avez perdu, utilisez iTunes pour le restaurer à l'aide de la dernière sauvegarde de l'appareil.

Microsoft Direct Push

Le serveur Exchange livre automatiquement le courrier électronique, les contacts et les événements de calendrier sur l'iPhone et l'iPad Wi-Fi + 3G si une connexion de données cellulaire ou Wi-Fi est accessible. L'iPod touch et l'iPad Wi-Fi ne sont pas dotés de capacités pour la connexion cellulaire ; ils ne reçoivent donc les notifications push que lorsqu'ils sont actifs et connectés à un réseau Wi-Fi.

Découverte automatique Microsoft Exchange

Le service de découverte automatique d'Exchange Server 2007 est pris en charge. Lorsque vous configurez manuellement un appareil, le service de découverte automatique utilise votre adresse électronique et votre mot de passe pour déterminer automatiquement les informations de serveur Exchange correctes. Pour en savoir plus sur l'activation du service de découverte automatique, consultez http://technet.microsoft.com/fr-fr/library/cc539114.aspx.

Liste d'adresses globale de Microsoft Exchange

L'iPhone, l'iPod touch et l'iPad extraient les informations de contact de l'annuaire d'entreprise du serveur Exchange de votre entreprise. Vous pouvez accéder à l'annuaire lorsque vous réalisez une recherche parmi les contacts et l'on y accède automatiquement pour compléter des adresses électroniques lors de la saisie.

Fonctionnalités ActiveSync Exchange complémentaires prises en charge

En plus des caractéristiques et fonctionnalités déjà décrites, l'iPhone OS prend en charge :

- la création d'invitations à des événements en calendrier (grâce à Microsoft Exchange 2007, vous pouvez également consulter l'état des réponses à vos invitations) ;
- le réglage de l'état Libre, Occupé, Tentative ou Absent pour vos événements de calendrier ;
- la recherche de messages électroniques sur le serveur (requiert Microsoft Exchange 2007) ;
- l'authentification client Exchange ActiveSync par certificat.

Fonctionnalités ActiveSync Exchange non prises en charge

Toutes les fonctionnalités d'Exchange ne sont pas prises en charge. Les fonctionnalités suivantes, par exemples, ne le sont pas :

- Gestion des dossiers
- Ouverture de liens pointant vers des documents stockés sur des serveurs Sharepoint dans des messages électroniques
- Synchronisation de tâches
- Définition d'un message de réponse automatique d'absence
- Marquage de messages pour suivi ultérieur

VPN

L'iPhone OS fonctionne avec les serveurs VPN qui prennent en charge les protocoles et méthodes d'authentification suivants :

- L2TP/IPSec avec authentification des utilisateurs par mot de passe MS-CHAPV2, RSA SecurID et CryptoCard et authentification des ordinateurs par secret partagé.
- PPTP avec authentification des utilisateurs par mot de passe MS-CHAPV2, RSA SecurID et CryptoCard.
- Cisco IPSec avec authentification des utilisateurs par mot de passe, RSA SecurID ou CryptoCard et authentification des ordinateurs par secret partagé et certificats. Consultez l'Annexe A pour voir la liste des serveurs VPN Cisco compatibles et pour obtenir des recommandations sur la configuration.

Cisco IPSec avec l'authentification par certificat prend en charge le VPN sur demande pour les domaines indiqués lors de la configuration. Consultez « Réglages VPN » à la page 38 pour en savoir plus.

Sécurité réseau

L'iPhone OS prend en charge les normes de sécurité de mise en réseau sans fil 802.11i suivantes, comme défini par la Wi-Fi Alliance :

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

De plus, l'iPhone OS prend en charge les méthodes d'authentification 802.1X pour réseaux WPA Enterprise et WPA2 Enterprise suivantes :

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

Certificats et identités

L'iPhone, l'iPod touch et l'iPad peuvent utiliser des certificats X.509 avec des clés RSA. Les extensions .cer, .crt et .der sont reconnues. Safari, Mail, VPN et d'autres applications réalisent des évaluations de chaîne de certificat.

Utilisez des fichiers P12 (norme PKCS #12) qui ne contiennent qu'une identité. Les extensions .p12 et .pfx sont reconnues. Lorsqu'une identité est installée, l'utilisateur est invité à saisir la phrase clé qui la protège.

Vous pouvez installer manuellement les certificats nécessaires pour établir la chaîne de certificat vers un certificat racine ou en utilisant les profils de configuration. Il n'est pas nécessaire d'ajouter les certificats racine qu'Apple a placés sur l'appareil. Pour afficher la liste des racines système préinstallées, consultez l'article du support d'Apple à l'adresse http://support.apple.com/kb/HT3580?locale=fr_FR.

Les certificats sont installables de façon sécurisée en mode OTA par le biais du protocole SCEP. Consultez « Vue d'ensemble du processus d'inscription et de configuration authentifié » à la page 24 pour en savoir plus.

Comptes de messagerie

L'iPhone, l'iPod touch et l'iPad prennent en charge les solutions de courrier électronique compatibles IMAP4 et POP3 standard de l'industrie sur une série de plate-formes serveur, notamment Windows, UNIX, Linux et Mac OS X. Vous pouvez également utiliser le protocole IMAP pour accéder au courrier électronique des comptes Exchange en plus du compte Exchange que vous utilisez avec la technologie Push directe.

Si un utilisateur effectue une recherche parmi ses courriers électroniques, il se voit proposé de poursuivre la recherche sur le serveur de messagerie. Ce procédé fonctionne avec Microsoft Exchange Server 2007 ainsi qu'avec la plupart des comptes IMAP.

Les informations du compte de messagerie de l'utilisateur, notamment l'identifiant d'utilisateur Exchange et son mot de passe, sont stockées de façon sécurisée sur l'appareil.

Serveurs LDAP

L'iPhone, l'iPod touch et l'iPad récupèrent les coordonnées depuis les annuaires d'entreprise de serveurs LDAPv3 dans votre entreprise. Vous pouvez accéder aux annuaires lors de la recherche parmi les contacts. Ces derniers sont automatiquement accédés pour compléter les adresses électroniques au fur et à mesure que vous les saisissez.

Serveurs CalDAV

L'iPhone, l'iPod touch et l'iPad synchronisent les données de calendrier avec le serveur CalDAV de votre entreprise. Les modifications apportées au calendrier sont régulièrement actualisées entre l'appareil et le serveur.

Il vous est également possible de vous abonner à des calendriers publiés en lecture seule, par exemple des calendriers de jours fériés ou l'emploi du temps d'un collègue.

La création et l'envoi de nouvelles invitations de calendrier depuis un appareil ne sont pas pris en charge pour les comptes CalDAV.

Ressources supplémentaires

En plus de ce guide, les publications et sites web suivants fournissent des informations utiles :

- page web de l'iPhone en entreprise à l'adresse www.apple.com/fr/iphone/enterprise ;
- La page iPad en entreprise, à l'adresse : www.apple.com/fr/ipad/business/
- vue d'ensemble des produits Exchange à l'adresse http://technet.microsoft.com/fr-fr/library/bb124558.aspx ;
- déploiement d'Exchange ActiveSync à l'adresse http://technet.microsoft.com/fr-fr/library/aa995962.aspx ;
- Bibliothèque de documentation technique Exchange 2003 à l'adresse http://technet.microsoft.com/fr-fr/library/bb123872(EXCHG.65).aspx ;
- Gestion de la sécurité Exchange ActiveSync à l'adresse http://technet.microsoft.com/fr-fr/library/bb232020(EXCHG.80).aspx ;
- page web « Wi-Fi for Enterprise » à l'adresse www.wi-fi.org/enterprise.php (en anglais) ;
- connectivité VPN iPhone pour les appareils de sécurité adaptatifs Cisco (ASA) à l'adresse www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html.
- « *Guide de l'utilisateur de iPhone* », disponible au téléchargement à l'adresse www.apple.com/fr/support/iphone/ Pour visualiser le guide sur l'iPhone, touchez le signet « Guide de l'utilisateur iPhone » dans Safari ou rendez-vous à la page http://support.apple.com/fr_FR/manuals/#iphone.
- visite guidée de l'iPhone, à l'adresse http://www.apple.com/fr/iphone/guidedtour/ ;
- « *Guide de l'utilisateur iPod touch* », disponible au téléchargement à l'adresse www.apple.com/fr/support/ipodtouch Pour visualiser le guide sur l'iPod touch, touchez le signet « Guide de l'utilisateur iPod touch » dans Safari ou rendez-vous à la page http://support.apple.com/fr_FR/manuals/#ipodtouch
- visite guidée de l'iPod touch, à l'adresse www.apple.com/fr/ipodtouch/guidedtour/ ;
- « *Guide de l'utilisateur iPad* », disponible au téléchargement à l'adresse www.apple.com/fr/support/ipad/. Pour visualiser le guide sur l'iPad sur l'iPad, touchez le signet « Guide de l'utilisateur » dans Safari ou rendez-vous à la page http://support.apple.com/fr_FR/manuals/#ipad.
- visite guidée de l'iPad, à l'adresse www.apple.com/ipad/guided-tours/

Déploiement de l'iPhone et de l'iPod touch

1

Le présent chapitre fournit une vue d'ensemble de la manière de déployer l'iPhone, l'iPod touch et l'iPad dans votre entreprise.

L'iPhone, l'iPod touch et l'iPad sont conçus de manière à s'intégrer facilement aux systèmes de votre entreprise, notamment avec Microsoft Exchange 2003 et 2007, les réseaux sans fil 802.1X sécurisés et les réseaux VPN IPSec Cisco. Comme pour toutes les solutions d'entreprise, une bonne planification et une bonne connaissance des options de déploiement dont vous disposez rendent le déploiement plus facile et plus efficace, tant pour vous que pour vos utilisateurs.

Lorsque vous planifiez le déploiement de l'iPhone, de l'iPod touch et de l'iPad, étudiez les questions suivantes :

- Comment activer les iPhone et iPad (modèles Wi-Fi + 3G) de votre entreprise pour profiter de votre forfait mobile ?
- À quels services, données et applications du réseau entreprise les utilisateurs doivent-ils accéder ?
- Quels règlements voulez-vous mettre en place sur les appareils pour protéger les données confidentielles de l'entreprise ?
- Voulez-vous configurer les appareils manuellement un à un ou utiliser un processus optimisé pour la configuration d'un vaste parc ?

Les spécificités de l'environnement, des règlements informatiques, de l'opérateur de télécommunication sans fil et de vos besoins en matière d'informatique et de communication de votre entreprise influencent la manière dont vous définissez votre stratégie de déploiement.

Activation d'appareils

Chaque iPhone doit être activé auprès de votre opérateur de télécommunication sans fil pour donner et recevoir des appels, envoyer des messages de texte ou se connecter au réseau de données cellulaire. Prenez contact avec votre opérateur pour connaître les tarifs voix et données et obtenir des instructions sur l'activation pour les clients privés et professionnels.

Vous ou vos utilisateurs devez installer une carte SIM dans l'iPhone. Une fois que la carte SIM est installée, l'iPhone doit être connecté à un ordinateur sur lequel iTunes est installé pour achever le processus d'activation. Si la carte SIM est déjà activée, l'iPhone est prêt pour une utilisation immédiate. À défaut, iTunes vous guide dans le processus d'activation d'une nouvelle ligne de service.

L'iPad doit être connecté à un ordinateur disposant d'iTunes afin d'activer l'appareil. Aux États-Unis, pour les modèles iPad Wi-Fi + 3G, vous pouvez souscrire et gérer (ou annuler) votre forfait données AT&T à l'aide de l'iPad. Accédez à Réglages > Données cellulaires > Visualiser le compte. Si l'iPad est déverrouillé, vous pouvez utiliser l'opérateur que vous voulez. Contactez votre opérateur pour configurer un compte et obtenir une carte micro SIM compatible. Aux États-Unis, les cartes micro SIM compatibles avec AT&T sont incluses avec l'iPad Wi-Fi + 3G.

Bien qu'il n'y ait pas service cellulaire ni de carte SIM pour l'iPod touch et l iPad Wi-Fi, ils doivent aussi être connectés à un ordinateur équipé d'iTunes pour l'activation.

iTunes étant obligatoire pour achever le processus d'activation, vous devez d'abord choisir entre installer iTunes sur le Mac ou le PC de chaque utilisateur ou procéder à l'activation de chaque appareil avec votre propre installation d'iTunes.

Après l'activation, iTunes n'est plus requis pour pouvoir utiliser l'appareil avec vos systèmes d'entreprise, mais il est nécessaire pour synchroniser de la musique, de la vidéo et les signets des navigateurs web avec un ordinateur. Il est aussi requis pour télécharger et installer des mises à jour de logiciels pour des appareils, et pour installer vos applications d'entreprise.

Pour en savoir plus sur l'activation des appareils et l'utilisation d'iTunes, consultez le chapitre 4.

Préparation de l'accès à des services réseau et des données d'entreprise

Le logiciel iPhone OS 3.x permet d'utiliser du courrier électronique sécurisé, des contacts et des calendriers push avec votre solution Microsoft Exchange Server 2003 ou 2007, ainsi que la recherche globale d'adresses, l'effacement à distance et l'application de règlements de codes des appareils. Il permet également aux utilisateurs de se connecter de manière sécurisée à des ressources d'entreprise via des réseaux sans fil WPA Enterprise et WPA2 Enterprise utilisant l'authentification sans fil 802.1X et/ou par VPN à l'aide des protocoles PPTP, LT2P sur IPSec ou Cisco IPSec.

Si votre entreprise n'utilise pas Microsoft Exchange, vos utilisateurs peuvent quand même employer l'iPhone ou l'iPod touch pour synchroniser du courrier électronique sans fil avec la plupart des serveurs et des services POP ou IMAP standard. En outre, ils peuvent utiliser iTunes pour synchroniser des événements de calendrier et des contacts de Mac OS X iCal et Carnet d'adresses ou de Microsoft Outlook sur un PC sous Windows. En ce qui concerne l'accès sans fil aux calendriers et aux annuaires, CalDAV et LDAP sont pris en charge.

Lorsque vous déterminez les services réseau auxquels vous voulez que les utilisateurs accèdent, consultez les informations de la section suivante.

Microsoft Exchange

L'iPhone communique directement avec votre serveur Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS). Exchange ActiveSync maintient une connexion entre le serveur Exchange et l'iPhone ou l'iPad Wi-Fi + 3G, de manière à ce que l'appareil soit actualisé instantanément lors de la réception d'un message électronique ou de l'invitation à une réunion. Ne possédant pas de connexion cellulaire, l'iPod touch et l'iPad Wi-Fi ne reçoivent les notifications push que lorsqu'ils sont activés et connectés à un réseau Wi-Fi.

Si votre entreprise prend en charge Exchange ActiveSync sur Exchange Server 2003 ou Exchange Server 2007, les services requis sont déjà en place. Pour Exchange Server 2007, assurez-vous que le rôle d'accès au client est installé. Pour Exchange Server 2003, assurez-vous qu'Outlook Mobile Access (OMA) est activé.

Si vous disposez d'un serveur Exchange mais que votre entreprise n'utilise pas encore Exchange ActiveSync, lisez attentivement les informations des sections suivantes.

Configuration du réseau

- Assurez-vous que le port 443 est ouvert sur le coupe-feu. Si votre entreprise utilise Outlook Web Access, le port 443 est probablement déjà ouvert.

- Vérifiez qu'un certificat de serveur est installé sur le serveur Exchange frontal et activez l'authentification de base uniquement dans les propriétés Méthode d'authentification afin d'exiger une connexion SSL à l'annuaire Microsoft Server ActiveSync de votre serveur IIS.
- Si vous utilisez un serveur Microsoft Internet Security and Acceleration (ISA), vérifiez qu'un certificat de serveur est installé et mettez à jour le serveur DNS public de manière à ce qu'il résolve correctement les connexions entrantes.
- Assurez-vous que le DNS de votre réseau renvoie une adresse unique et routable depuis l'extérieur au serveur Exchange ActiveSync tant pour les clients intranet que pour les clients Internet. Cela est obligatoire pour que les appareils puissent utiliser la même adresse IP pour communiquer avec le serveur lorsque les deux types de connexion sont actifs.
- Si vous utilisez un serveur ISA, créez un écouteur web ainsi qu'une règle de publication d'accès pour client web Exchange. Consultez la documentation de Microsoft pour obtenir des informations détaillées.
- Pour tous les coupe-feu et équipements réseau, définissez à 30 minutes le délai d'attente en cas de session inactive. Pour en savoir plus sur les intervalles de pulsations et de délai d'attente, consultez la documentation de Microsoft Exchange à l'adresse suivante : http://technet.microsoft.com/en-us/library/cc182270.aspx.

Configuration du compte Exchange

- Activez Exchange ActiveSync pour certains utilisateurs ou groupes à l'aide du service Active Directory. Ils sont activés par défaut sur tous les appareils mobiles au niveau organisationnel dans Exchange Server 2003 et Exchange Server 2007. Pour Exchange Server 2007, consultez la configuration des destinataires dans la console Exchange Management.
- Configurez les fonctionnalités, les règlements et les réglages en matière de sécurité des appareils mobiles à l'aide d'Exchange System Manager. Pour Exchange Server 2007, effectuez la configuration dans la console Exchange Management.
- Téléchargez et installez l'outil Microsoft Exchange ActiveSync Mobile Administration Web Tool, qui est nécessaire pour lancer une réinitialisation à distance. Pour Exchange Server 2007, une réinitialisation à distance peut également être lancée à l'aide d'Outlook Web Access ou de la console Exchange Management.

Réseaux WPA/WPA2 Enterprise

La prise en charge de WPA Enterprise et de WPA2 Enterprise permet de s'assurer que l'on accède aux réseaux sans fil d'entreprise de manière sécurisée sur l'iPhone, l'iPod touch et l'iPad. WPA/WPA2 Enterprise utilise le chiffrement AES à 128 bits, une méthode de chiffrement par blocs qui a fait ses preuves et qui confère à la protection des données d'entreprise un haut degré d'assurance.

Avec la prise en charge de l'authentification 802.1X, les appareils sous iPhone OS peuvent être intégrés dans une grande variété d'environnements de serveur RADIUS. Les méthodes d'authentification sans fil 802.1X, telles que EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 et LEAP, sont prises en charge.

Configuration d'un réseau WPA/WPA2 Enterprise

- Vérifiez que les équipements réseau sont compatibles et sélectionnez un type d'authentification (type EAP) pris en charge par l'iPhone, l'iPod touch et l'iPad. Assurez-vous que 802.1X est activé sur le serveur d'authentification et, si nécessaire, installez un certificat de serveur et assignez des permissions d'accès réseau aux utilisateurs et groupes.
- Configurez des points d'accès sans fil pour l'authentification 802.1X et saisissez les informations sur le serveur RADIUS correspondantes.
- Testez votre déploiement 802.1X avec un Mac ou un PC pour vous assurer que l'authentification RADIUS est configurée correctement.
- Si vous comptez utiliser l'authentification par certificats, assurez-vous que votre infrastructure à clé publique est configurée de manière à prendre en charge les certificats d'appareil et d'utilisateur avec le processus de distribution de clés correspondant.
- Vérifiez la compatibilité de vos formats de certificat avec l'appareil et votre serveur d'authentification. Pour en savoir plus sur les certificats, consultez « Certificats et identités » à la page 12.

Réseaux privés virtuels

L'accès sécurisé à des réseaux privés est pris en charge sur l'iPhone, l'iPod touch et l'iPad à l'aide des protocoles Cisco IPSec, L2TP sur IPSec et du protocole de réseau privé virtuel PPTP. Si votre organisation prend en charge l'un de ces protocoles, aucune configuration réseau ni d'application de tierce partie n'est nécessaire pour utiliser vos appareils avec votre infrastructure VPN.

Les déploiements Cisco IPSec peuvent bénéficier de l'authentification par certificats à l'aide de certificats x.509 standard de l'industrie. L'authentification par certificats vous permet également de bénéficier des connexions VPN sur demande, assurant un accès sans fil continu et sécurisé au réseau de votre entreprise.

Pour l'authentification par jetons à deux facteurs, l'iPhone OS prend en charge RSA SecurID et CryptoCard. Les utilisateurs saisissent leur PIN et leur mot de passe à utilisation unique généré par jeton directement sur leur appareil lorsqu'ils établissent une connexion VPN. Consultez l'Annexe A pour voir la liste des serveurs VPN Cisco compatibles et pour obtenir des recommandations sur la configuration.

L'iPhone, l'iPod touch et l'iPad prennent également en charge l'authentification par secret partagé pour les déploiements Cisco IPSec et L2TP/IPSec ainsi que MS-CHAPv2 pour l'authentification par nom d'utilisateur et mot de passe simple.

La configuration automatique de proxy VPN (PAC et WPAD) est aussi prise en charge. Elle vous permet de préciser les réglages du serveur proxy pour accéder à des URL spécifiques.

Instructions pour la configuration d'un VPN

- Le système d'exploitation iPhone OS s'intègre à la plupart des réseaux VPN existants. La configuration nécessaire pour que les appareils sous iPhone OS puissent accéder à votre réseau doit donc être minimale. La meilleure manière de préparer le déploiement consiste à vérifier si les protocoles VPN et les méthodes d'authentification utilisés par votre entreprise sont pris en charge par l'iPhone.
- Assurez-vous que vos concentrateurs VPN sont bien compatibles avec les normes. Il est aussi recommandé de vérifier le chemin d'authentification jusqu'à votre serveur RADIUS ou d'authentification pour vous assurer que les normes prises en charge par l'iPhone OS sont activées au sein de votre implémentation.
- Vérifiez auprès de votre fournisseur de solutions que les derniers correctifs de sécurité et programmes internes sont bien installés sur vos logiciels et votre équipement.
- Si vous voulez configurer des réglages de proxy propres à des URL, placez un fichier PAC sur un serveur web accessible avec les réglages VPN de base, puis assurez-vous qu'il est transféré avec un type MIME d'application/x-ns-proxy-autoconfig. Une autre solution consiste à configurer votre DNS ou DHCP afin de fournir l'emplacement d'un fichier WPAD sur un serveur accessible de la même manière.

Courrier électronique IMAP

Si vous n'utilisez pas Microsoft Exchange, vous pouvez quand même implémenter une solution de courrier électronique à base de normes sécurisée à l'aide de tout serveur de courrier électronique prenant en charge IMAP et configuré pour exiger l'authentification des utilisateurs et SSL. Par exemple, vous pouvez accéder au courrier électronique Lotus Notes/Domino ou Novell GroupWise en utilisant cette technique. Les serveurs de messagerie peuvent se trouver au sein d'un sous-réseau de zone démilitarisée, derrière un coupe-feu d'entreprise, ou dans les deux.

Avec SSL, l'iPhone OS prend en charge le chiffrement 128 bits et les certificats X.509 émis par les principales autorités de certificat. Il prend également en charge des méthodes d'authentification informatiques fortes actuelles, notamment MD5 Challenge-Response et NTLMv2.

Instructions pour la configuration d'un réseau IMAP

- Pour une meilleure protection, installez un certificat numérique émis par une autorité de certificat (AC) de confiance sur le serveur. L'installation d'un certificat émis par une AC est essentielle dans le processus de vérification de votre serveur proxy en tant qu'entité de confiance au sein de l'infrastructure de votre entreprise. Voir « Réglages de références » à la page 42 pour en savoir plus sur l'installation de certificats sur l'iPhone.

- Pour autoriser les appareils sous iPhone OS à relever le courrier électronique sur votre serveur, ouvrez le port 993 dans le coupe-feu et assurez-vous que le serveur proxy est configuré de manière à utiliser IMAP sur SSL.
- Pour autoriser les appareils à envoyer du courrier électronique, le port 587, 465 ou 25 doit être ouvert. Le port 587, qui est utilisé en premier, constitue le meilleur choix.

Annuaires LDAP

L'iPhone OS vous permet d'accéder aux serveurs d'annuaires LDAP et fournit un annuaire d'adresses global et des informations similaires à la Liste d'adresses globale de Microsoft Exchange.

Si vous configurez un compte LDAP sur l'appareil, ce dernier recherche alors l'attribut `namingContexts` au niveau root du serveur pour identifier la base de recherche par défaut. L'étendue de recherche est définie par défaut sur l'arborescence (Sous-arbre).

Calendriers CalDAV

La prise en charge CalDAV d'iPhone OS permet d'assurer l'organisation du temps et des calendriers globaux pour les entreprises qui n'utilisent pas Microsoft Exchange. L'iPhone OS fonctionne avec les serveurs de calendrier prenant en charge la norme CalDAV.

Abonnements aux calendriers

Si vous comptez publier des calendriers en lecture seule incluant des événements communs, tels que les vacances ou des événements particuliers programmés, les appareils sous iPhone OS peuvent s'abonner à des calendriers et afficher ainsi leurs renseignements en plus de leurs calendriers Microsoft Exchange et CalDAV. L'iPhone OS manipule les fichiers de calendrier au format iCalendar (.ics) standard.

Un moyen facile pour distribuer les calendriers auxquels vos utilisateurs se sont abonnés consiste à envoyer l'URL complète par SMS ou par courrier électronique. Lorsque l'utilisateur tapote sur le lien, l'appareil l'invite à s'abonner au calendrier spécifié.

Applications d'entreprise

Si vous avez l'intention de déployer des applications iPhone OS d'entreprise, installez-les sur vos appareils à l'aide d'« Utilitaire de configuration iPhone » pour Mac OS X ou d'iTunes pour Mac ou Windows. Une fois que vous avez déployé des applications sur des appareils d'utilisateurs, la mise à jour de celles-ci sera plus aisée si iTunes est installé sur le Mac ou le PC de chaque utilisateur.

Protocole de vérification en ligne de certificat (OSCP - Online Certificate Status Protocol)

Lorsque vous fournissez des certificats numériques pour les appareils sous iPhone OS, pensez à les émettre de façon à ce qu'ils soient compatibles avec le protocole OCSP. Ainsi, l'appareil demande à votre serveur OCSP si le certificat a été révoqué avant de l'utiliser.

Définition de règlements de code d'appareil

Une fois définis les services et les données réseau auxquels vos utilisateurs doivent avoir accès, vous devez choisir les règlements de code d'appareil à mettre en place.

Pour les entreprises dont les réseaux, systèmes ou applications n'exigent pas de mot de passe ni de jeton d'authentification, il est recommandé de définir des codes sur les appareils. Si vous utilisez l'authentification par certificats pour un réseau 802.1X ou un VPN Cisco IPSec, ou si votre application d'entreprise enregistre vos références d'ouverture de session, vous devez obliger les utilisateurs à définir un code d'appareil avec un délai d'attente court pour que les appareils se verrouillent rapidement en cas de perte ou de vol.

Vous pouvez définir les règlements sur l'iPhone, l'iPod touch et l'iPad de l'une des deux manières. Si l'appareil est configuré pour accéder à un compte Microsoft Exchange, les stratégies Exchange ActiveSync sont transmises à l'appareil à travers une connexion sans fil. Cela vous permet d'appliquer et de mettre à jour les règlements sans intervention de l'utilisateur. Pour en savoir plus sur les règlements EAS, consultez « Règlements Exchange ActiveSync pris en charge » à la page 9.

Si vous n'utilisez pas Microsoft Exchange, vous pouvez définir des règlements similaires sur vos appareils en créant des profils de configuration. Lorsque vous modifiez un règlement, les utilisateurs doivent installer le profil mis à jour que vous leur adressez par le biais d'« Utilitaire de configuration iPhone ». Pour en savoir plus sur les règlements de code d'appareil, consultez « Réglages relatifs au code » à la page 35.

Si vous utilisez Microsoft Exchange, vous pouvez également compléter vos règlements EAS en utilisant les règlements de configuration. Vous accédez par exemple à des règlements qui ne sont pas disponibles dans Microsoft Exchange 2003 ou qui vous permettent de définir des règlements spécifiques pour les appareils sous iPhone OS.

Configuration d'appareils

Vous devez ensuite choisir la manière dont vous allez configurer chaque iPhone, iPod touch ou iPad. Cette décision dépend en partie du nombre d'appareils que vous allez devoir déployer et gérer. Si le nombre d'appareils est peu élevé, il peut cependant s'avérer plus simple, pour vous ou vos utilisateurs, de configurer chaque appareil manuellement. Cela implique d'utiliser l'appareil pour définir les réglages de chaque compte de courrier électronique, les réglages Wi-Fi et les informations de configuration VPN. Consultez le chapitre 3 pour en savoir plus sur la configuration manuelle.

Si vous déployez un grand nombre d'appareils ou si les réglages de courrier électronique, réglages réseau et certificats à installer sont nombreux, vous voudrez sans doute configurer les appareils en créant et distribuant des profils de configuration. Les profils de configuration permettent de charger rapidement des réglages et des informations d'autorisation sur un appareil. Certains réglages VPN et Wi-Fi ne peuvent être définis qu'à l'aide d'un profil de configuration et, si vous n'utilisez pas Microsoft Exchange, vous devez faire appel à un profil de configuration pour définir des règlements de code d'appareil.

Vous pouvez chiffrer et signer les profils de configuration, ce qui vous permet de limiter leur usage à un appareil donné et empêche quiconque de modifier les réglages inclus dans un profil. Vous avez également la possibilité de marquer un profil comme étant verrouillé à un appareil de sorte qu'une fois installé, personne ne peut le supprimer sans passer par la destruction de toutes les données de l'appareil ou, le cas échéant, introduire le code d'un administrateur.

Que vous configuriez les appareils manuellement ou à l'aide de profils de configuration, vous devez également choisir entre configurer les appareils vous-même ou déléguer cette tâche à vos utilisateurs. Votre choix va dépendre de l'emplacement de vos utilisateurs, du règlement de votre entreprise en matière de gestion de l'équipement informatique par les utilisateurs eux-mêmes et de la complexité de la configuration des appareils que vous comptez déployer. Les profils de configuration sont idéaux dans les grandes entreprises, pour les employés qui travaillent à distance ou pour les utilisateurs qui ne sont pas capables de configurer leurs appareils.

Si vous voulez que les utilisateurs activent leur appareil eux-mêmes ou s'ils doivent installer ou mettre à jour des applications d'entreprise, iTunes doit être installé sur le Mac ou le PC de chaque utilisateur. iTunes est également nécessaire pour les mises à jour de logiciels de l'iPhone OS, ce qui constitue un point important si vous choisissez de ne pas distribuer iTunes à vos utilisateurs. Pour obtenir en savoir plus sur le déploiement d'iTunes, consultez le chapitre 4.

Inscription et configuration en mode OTA

L'*inscription* est le processus d'authentification d'un appareil et d'un utilisateur afin d'automatiser le processus de distribution des certificats. Les certificats numériques fournissent de nombreux avantages aux utilisateurs. Ils permettent d'authentifier l'accès à des services clé professionnels, tels que Microsoft Exchange ActiveSync, les réseaux sans fil WPA2 Enterprise et les connexions VPN en entreprise. L'authentification par certificat permet également l'utilisation du VPN sur demande pour l'accès direct aux réseaux en entreprise.

Outre les fonctionnalités d'inscription en mode OTA pour délivrer des certificats pour l'infrastructure de clé publique (PKI, Public Key Infrastructure) de votre entreprise, vous pouvez également déployer des profils de configuration d'appareil. Cela permet de limiter aux seuls utilisateurs de confiance d'accéder aux services de l'entreprise et de s'assurer que les appareils de ces utilisateurs sont configurés en accord avec votre règlement informatique. Dans la mesure où les profils de configuration peuvent être à la fois chiffrés et verrouillés, il est impossible de supprimer leurs réglages, de les modifier ou de les partager avec autrui. Ces fonctionnalités vous sont proposées dans le cadre du processus en mode OTA décrit plus loin, et sont en outre accessibles par le biais d'« Utilitaire de configuration iPhone » pour paramétrer des appareils branchés sur l'ordinateur servant à votre administration. Consultez le chapitre 2 pour en savoir plus sur l'usage d'« Utilitaire de configuration iPhone ».

La mise en service de l'inscription et de la configuration en mode OTA impose le développement et l'intégration de services d'authentification, d'annuaire et de certificats. Vous pouvez réaliser le déploiement par le biais de services web standard puis, une fois en place, permettre à vos utilisateurs de configurer leur appareil de façon sécurisée en s'authentifiant.

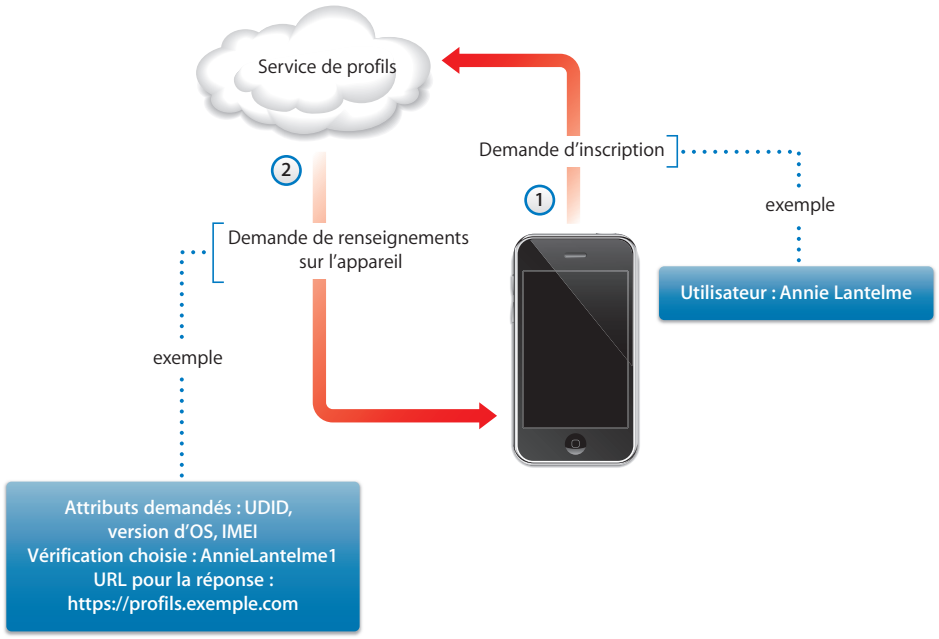
Vue d'ensemble du processus d'inscription et de configuration authentifié

Pour mettre en place ce processus, vous devez créer votre propre *service de distribution de profils* chargé d'accepter les connexions HTTP, d'authentifier les utilisateurs, de créer les profils mobileconfig et de gérer le processus principal décrit dans cette rubrique.

Vous devez également demander à une AC (Autorité de Certification) de produire les références de l'appareil et de vous les communiquer par SCEP (Simple Certificate Enrollment Protocol). Pour retrouver les liens vers les rubriques sur PKI, SCEP, ainsi que les rubriques connexes, consultez la section « Autres ressources » à la page 29.

Le diagramme qui suit décrit le processus d'inscription et de configuration que l'iPhone prend en charge.

Phase 1 - Lancement de l'inscription

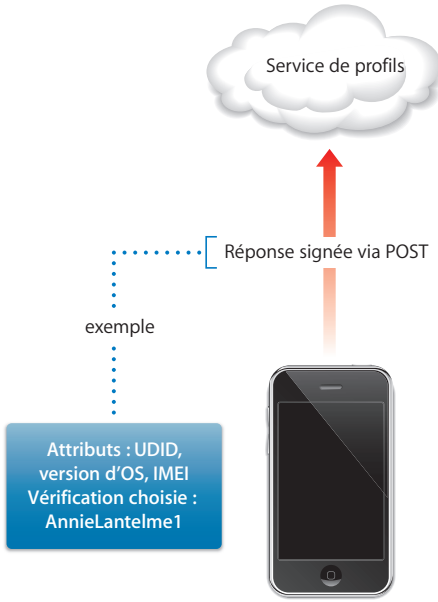


Phase 1 – Lancement de l'inscription : à l'aide de Safari, l'utilisateur accède à l'URL du service de distribution de profils que vous avez créé. Vous pouvez distribuer cette URL par SMS ou par courrier électronique. Cette étape constitue la demande d'inscription, représentée par l'étape 1 dans le graphique, au cours de laquelle vous devez confirmer l'identité de l'utilisateur. Cette authentification peut constituer une simple authentification de base, mais vous pouvez aussi la faire transiter par vos services d'annuaire.

En étape 2, votre service transmet en réponse un profil de configuration (.mobileconfig). Cette réponse compile la liste des attributs que l'appareil doit fournir en autre réponse, et une clé prépartagée (appelée requête ou vérification) pouvant éventuellement contenir l'identité de l'utilisateur de façon à pouvoir personnaliser, plus en aval de cette procédure, le processus de configuration pour chaque utilisateur. Les attributs d'appareil que le service peut demander sont la version d'iPhone OS, l'identifiant de l'appareil (l'adresse MAC), le type de produit (l'iPhone 3GS renvoie à iPhone2,1), l'identifiant du téléphone (IMEI) et les renseignements sur la SIM (l'ICCID).

Pour retrouver un exemple de profil de configuration illustrant cette phase, consultez « Échantillon de réponse du serveur (phase 1) » à la page 92.

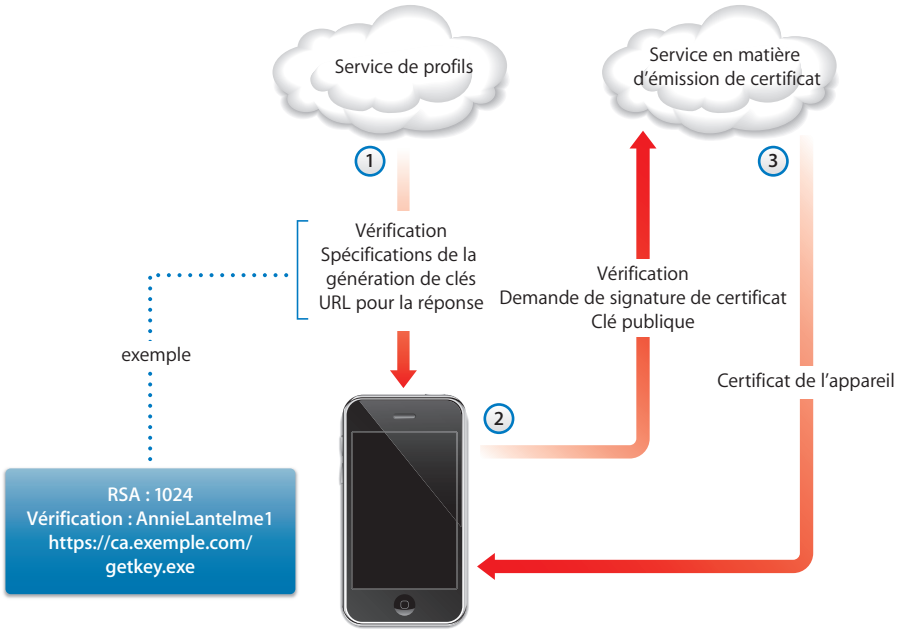
Phase 2 - Authentification de l'appareil



Phase 2 – Authentification de l'appareil : une fois que l'utilisateur a accepté l'installation du profil reçu en phase 1, l'appareil recherche les attributs demandés, ajoute la réponse de vérification (si elle a été fournie) et signe la réponse à l'aide de l'identité intégrée à l'appareil (c'est-à-dire le certificat émis par Apple), puis la retransmet au serveur à l'aide d'une méthode Post HTTP.

Pour retrouver un exemple de profil de configuration illustrant cette phase, consultez « Échantillon de réponse de l'appareil (phase 2) » à la page 93.

Phase 3 - Installation du certificat de l'appareil



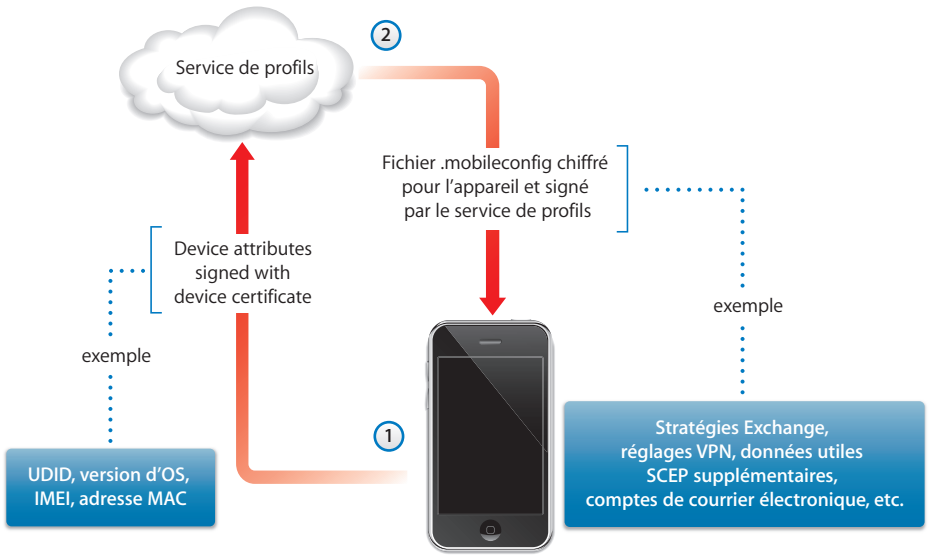
Phase 3 – Installation du certificat : en étape 1, le service de distribution de profils en spécifiant les instructions pour que l'appareil génère une clé (RSA 1024) et l'endroit où il doit la renvoyer à travers SCEP (Simple Certificate Enrollment Protocol) pour obtenir la certification.

En étape 2, la demande SCEP doit être gérée automatiquement, en se servant de la vérification en réponse issue du paquet SCEP pour authentifier la demande.

En troisième étape, l'AC répond par un certificat de chiffrement pour l'appareil.

Pour retrouver un exemple de profil de configuration illustrant cette phase, consultez « Échantillon de réponse du serveur (phase 3) avec spécifications SCEP » à la page 94.

Phase 4 - Configuration de l'appareil



Phase 4 – Configuration de l'appareil : pour commencer, l'appareil répond par la liste des attributs, laquelle doit être signée à l'aide du certificat de chiffrement fourni par l'AC au cours de la phase précédente.

En étape 2, le service de profils répond par un fichier .mobileconfig chiffré, installé automatiquement. Le service de profil doit avoir signé ce fichier .mobileconfig. Son certificat SSL peut au besoin servir dans ce cas.

En plus des réglages généraux, ce profil de configuration doit également définir les règlements d'entreprise que vous voulez imposer et doit correspondre à un profil verrouillé de sorte que l'utilisateur ne puisse pas le supprimer de l'appareil. Le profil de configuration peut renfermer d'autres requêtes d'inscription à des identités via SCEP, lesquelles s'exécutent lorsque le profil s'installe.

De la même façon, lorsqu'un certificat installé via SCEP expire ou n'est pas validé, l'appareil demande à l'utilisateur de mettre à jour le profil. Lorsque l'utilisateur autorise la requête, l'appareil répète le processus ci-dessus pour obtenir un nouveau certificat et un nouveau profil.

Pour retrouver un exemple de profil de configuration illustrant cette phase, consultez « Échantillon de réponse de l'appareil (phase 4) » à la page 96.

Autres ressources

- PKI de certificats numériques pour VPN IPSec à l'adresse https://cisco.hosted.jivesoftware.com/docs/DOC-3592 (en anglais)
- Infrastructure à clés publiques à l'adresse http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques
- Spécifications du protocole SCEP IETF à l'adresse http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt (en anglais)

D'autres informations et ressources utiles sur l'iPhone et l'iPod touch en entreprise sont disponibles à l'adresse www.apple.com/fr/iphone/enterprise et www.apple.com/fr/ipad/business.

Création et déploiement de profils de configuration

2

Les profils de configuration définissent la manière dont l'iPhone, l'iPod touch et l'iPad fonctionnent avec les systèmes de votre entreprise.

Ces profils correspondent à des fichiers XML contenant les règlements et les restrictions de sécurité de l'appareil, les données de configuration de VPN, les réglages Wi-Fi, les comptes de courrier électronique et de calendrier, ainsi que les références permettant à l'iPhone, l'iPod touch et l'iPad de fonctionner avec les systèmes de votre enterprise.

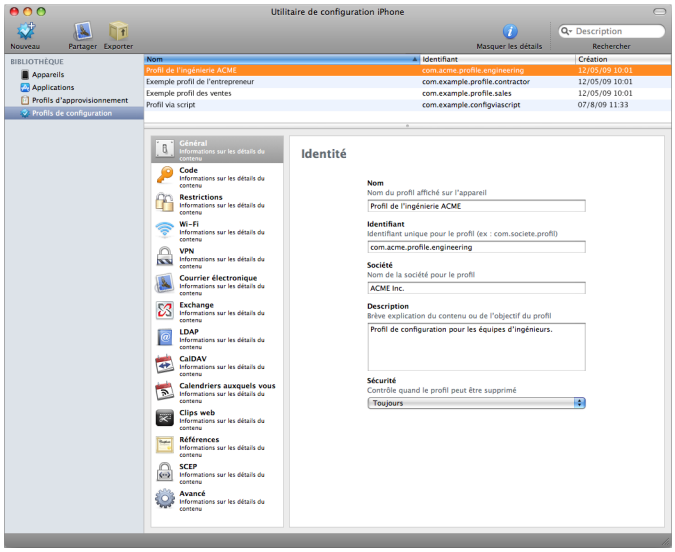
Vous avez la possibilité d'installer les profils de configuration sur des appareils branchés sur un port USB d'un ordinateur par le biais d'« Utilitaire de configuration iPhone ». Vous pouvez également distribuer ces profils de configuration par courrier électronique ou à travers une page web. Lorsque des utilisateurs ouvrent la pièce jointe à un message électronique ou téléchargent le profil sur leur appareil à l'aide de Safari, ils sont invités à lancer le processus d'installation.

Si vous préférez ne pas créer ni distribuer de profils de configuration, vous pouvez configurer les appareils manuellement. Pour en savoir plus, reportez-vous au Chapitre 3.

À propos d'« Utilitaire de configuration iPhone »

« Utilitaire de configuration iPhone » vous permet, en toute simplicité, de créer, chiffrer et installer des profils de configuration, de contrôler et installer des profils d'approvisionnement et des applications autorisées, ainsi que de capturer des renseignements sur les appareils de capture, notamment leurs historiques de console. Lorsque vous exécutez le programme d'installation d'« Utilitaire de configuration iPhone », l'installation s'effectue dans /Applications/Utilitaires/ sous Mac OS X, ou dans Programmes\Utilitaire de configuration iPhone\ sous Windows.

Lorsque vous ouvrez « Utilitaire de configuration iPhone », une fenêtre semblable à celle ci-dessous apparaît.



Le contenu de la section principale de cette fenêtre change en fonction des éléments sélectionnés dans la barre latérale.

La barre latérale affiche la bibliothèque, qui contient les catégories suivantes :

- *Appareils* affiche la liste des iPhone et iPod touch connectés à votre ordinateur.
- *Applications* affiche la liste des applications qui sont disponibles pour l'installation sur les appareils rattachés à votre ordinateur. Un profil d'approvisionnement peut s'avérer nécessaire pour exécuter une application sur un équipement.
- *Profils d'approvisionnement* affiche la liste des profils qui permettent l'utilisation de l'appareil pour le développement iPhone OS, tel qu'il est autorisé par l'Apple Developer Connection. Pour obtenir des informations, consultez le chapitre 5. Les profils d'approvisionnement permettent également aux appareils d'exécuter des applications professionnelles non distribuées par l'iTunes Store.

- *Profils de configuration* répertorie les profils de configuration créés précédemment, et vous permet de modifier les informations ou de créer une configuration que vous pouvez envoyer à un utilisateur ou installer sur un appareil branché.

La barre latérale contient également *Appareils connectés*, qui affiche des informations sur les appareils sous iPhone OS connectés au port USB de votre ordinateur. Des informations relatives à un appareil branché s'ajoutent automatiquement à la liste Appareils afin que vous puissiez les consulter à nouveau sans devoir reconnecter le dispositif. Après qu'un appareil ait été branché, vous pouvez également chiffrer les profils de sorte à ne les utiliser que sur cet appareil.

Lorsque qu'un appareil est branché, vous avez la possibilité de passer par « Utilitaire de configuration iPhone » afin d'installer les profils de configuration et les applications sur l'équipement en question. Consultez « Installation de profils de configuration à l'aide d'« Utilitaire de configuration iPhone » » à la page 44,« Installation d'applications à l'aide d'« Utilitaire de configuration iPhone » » à la page 72 et « Installation de profils d'approvisionnement à l'aide d'« Utilitaire de configuration iPhone » » à la page 71 pour en savoir plus.

Lorsqu'un appareil est connecté, vous pouvez également afficher des historiques Console et tout historique de panne grave. Il s'agit des mêmes historiques d'appareil que ceux qui sont disponibles pour l'affichage dans l'environnement de développement Xcode sous Mac OS X.

Création de profils de configuration

Le présent document fait appel aux termes *profil de configuration* et *donnée utile*. Un profil de configuration constitue un fichier intégral qui configure certains réglages (individuels ou multiples) pour un iPhone, un iPod touch ou un iPad. Une donnée utile représente une collection précise d'un certain type de réglages, tels que les réglages de VPN, au sein du profil de configuration.

Bien que vous puissiez créer un seul profil de configuration contenant toutes les données utiles nécessaires à votre entreprise, songez à créer un profil pour les certificats et un autre (ou plusieurs) pour les réglages afin de pouvoir mettre à jour et de distribuer les deux types d'informations séparément. Cela permet également aux utilisateurs de conserver les certificats déjà installés lorsqu'ils installent un nouveau profil contenant des réglages VPN ou de compte.

De nombreuses données utiles vous permettent d'indiquer les noms d'utilisateur et mots de passe. Le profil peut servir à plusieurs utilisateurs, mais si vous omettez ces informations, chacun doit alors saisir les informations manquantes une fois le profil installé. Si vous personnalisez le profil pour chaque utilisateur, et prévoyez dans ce but des mots de passe, vous devez distribuer le profil sous un format chiffré pour protéger son contenu. Pour en savoir plus, consultez « Installation de profils de configuration » à la page 44

Pour créer un profil de configuration, cliquez sur le bouton Nouveau dans la barre d'outils d'« Utilitaire de configuration iPhone ». Vous pouvez ajouter des données utiles au profil par le biais de la liste des données utiles. Vous devez ensuite modifier ces données en saisissant et en sélectionnant des options parmi celles qui apparaissent dans la sous-fenêtre de modification. Les champs obligatoires sont marqués d'une flèche rouge. Concernant certains réglages, comme les réglages Wi-Fi, vous pouvez cliquer sur le bouton Ajouter (+) pour ajouter des configurations. Pour supprimer une configuration, cliquez sur le bouton Supprimer (–) dans la sous-fenêtre de modification.

Pour modifier une donnée utile, sélectionnez l'élément de votre choix dans la liste des données utiles, cliquez sur le bouton Configurer, puis renseignez les champs tel qu'il est décrit ci-dessous.

Automatisation de la création de profils de configuration

Vous pouvez également automatiser la création des fichiers de configuration à l'aide d'AppleScript sur un Mac ou de scripts C# sous Windows. Pour voir les méthodes prises en charge et leur syntaxe, procédez comme suit :

- *Mac OS X* : utilisez Éditeur de scripts pour ouvrir le dictionnaire AppleScript concernant « Utilitaire de configuration iPhone ».
- *Windows* : utilisez Visual Studio pour voir les appels de méthode fournis par iPCUScripting.dll.

Pour exécuter un script, sur Mac, utilisez la commande Tell d'AppleScript. Sous Windows, passez le nom de script dans « Utilitaire de configuration iPhone » comme paramètre de ligne de commande.

Pour obtenir des exemples, consultez l'annexe C, « Exemples de scripts. »

Réglages généraux

Vous devez fournir à cet endroit le nom et l'identifiant du profil en question, et indiquer si les utilisateurs sont autorisés à supprimer le profil après qu'il ait été installé.

Le nom que vous spécifiez apparaît dans la liste des profils et est affiché sur l'appareil une fois que le profil de configuration est installé. Le nom ne doit pas nécessairement être unique, mais il est recommandé d'utiliser un nom évocateur identifiant le profil.

L'identifiant du profil, lui, doit être unique et doit suivre la forme com. *nom_de_l'entreprise.identifiant*, où *identifiant* décrit le profil.
(Par exemple, com.mycompany.homeoffice.)

L'identifiant est important car, une fois le profil installé, sa valeur est comparée aux profils qui se trouvent déjà sur l'appareil. Si l'identifiant est unique, les informations du profil sont ajoutées à l'appareil. Si l'identifiant correspond à un profil déjà installé, les informations du profil remplacent les réglages qui se trouvent déjà sur l'appareil, à part les réglages Exchange. Pour modifier un compte Exchange, le profil doit d'abord être supprimé manuellement de sorte que les données associées au compte soient éliminées.

Pour empêcher qu'un utilisateur supprime un profil installé sur un appareil, choisissez une option à partir du menu local Sécurité. L'option Avec autorisation vous permet d'indiquer le mot de passe d'autorisation permettant le retrait du profil de l'appareil. Si vous sélectionnez l'option Jamais, le profil peut se mettre à jour à une nouvelle version mais ne peut pas être supprimé.

Réglages relatifs au code

Utilisez cette donnée utile pour définir des règlements propres aux appareils si vous ne faites pas appel à celles relatives aux codes Exchange. Vous pouvez spécifier si un code est obligatoire pour pouvoir utiliser l'appareil mais également définir des caractéristiques du code et la fréquence à laquelle il doit être changé. Une fois le profil de configuration chargé, l'utilisateur est invité à saisir un code qui satisfait aux conditions des règlements sélectionnés. À défaut, le profil ne peut pas s'installer.

Si vous utilisez des règlements pour appareil et des règlements relatifs aux codes Exchange, les deux règlements sont alors fusionnés et ce sont les réglages les plus stricts qui sont appliqués. Pour en savoir plus sur les règlements Exchange ActiveSync pris en charge, consultez « Microsoft Exchange ActiveSync » à la page 8.

Les règlements suivants sont disponibles :

- *Exiger un code sur l'appareil :* oblige les utilisateurs à saisir un code avant d'utiliser l'appareil. À défaut, toute personne qui dispose de l'équipement peut accéder à l'ensemble de ses fonctions et données.
- *Accepter les valeurs simples :* permet aux utilisateurs d'utiliser des caractères consécutifs ou répétés dans leur code. Par exemple, les codes « 3333 » ou « DEFG » sont autorisés.
- *Exiger des valeurs alphanumériques :* requiert que le code contienne au moins une lettre.
- *Longueur minimum du mot de passe :* spécifie le nombre minimum de caractères qu'un code peut contenir.
- *Nombre minimum de caractères complexes :* nombre de caractères non alphanumériques (comme $, & et !) que le code doit contenir.
- *Durée maximum du code (en jours) :* oblige les utilisateurs à changer leur code à l'intervalle spécifié.
- *Verrouillage automatique (en minutes) :* si l'appareil n'est pas utilisé pendant ce temps, il se verrouille automatiquement. La saisie du code le déverrouille.
- *Historique de code :* tout nouveau code est refusé s'il correspond à un autre utilisé auparavant. Vous pouvez indiquer le nombre de codes mémorisés précédents dans le cadre de cette comparaison.
- *Délai de grâce pour le verrouillage de l'appareil :* précise la durée au cours de laquelle l'appareil peut encore être déverrouillé sans redemander le code.

- *Nombre maximum de tentatives :* détermine le nombre de tentatives de saisie du code autorisées avant que l'appareil ne soit mis en pause. Si vous ne voulez pas changer ce réglage à l'issue de six tentatives, l'appareil impose un délai d'attente avant toute autre essai. Ce délai d'attente augmente à chaque nouvelle tentative vaine. Après la onzième tentative vaine, toutes les données et tous les réglages sont effacés de l'appareil de manière sécurisée. Les délais d'attente de saisie du code commencent toujours après la sixième tentative, donc, si vous réglez cette valeur sur 6 ou moins, aucun délai d'attente n'est imposé et toutes les données et tous les réglages de l'appareil sont effacés lorsque le nombre de tentatives spécifié est atteint.

Réglages des restrictions

Faites appel à cette donnée utile pour préciser les fonctionnalités de l'appareil l'utilisateur est en droit d'exploiter.

- *Autoriser le contenu explicite :* si l'option est désactivée, le contenu musical ou vidéo réservé à un public averti acheté auprès de l'iTunes Store est masqué. Les éléments réservés à un public averti sont clairement indiqués, d'après les données procurées par leur fournisseur, par exemple un label musical, au moment de leur vente à travers l'iTunes Store.
- *Autoriser l'utilisation de Safari :* si cette option est décochée, le navigateur web Safari est désactivé et son icône retirée du menu principal. Elle empêche également l'utilisateur d'ouvrir des clips web.
- *Autoriser l'utilisation de YouTube :* si cette option est décochée, l'accès à YouTube est désactivé et l'icône de l'application est retirée du menu principal.
- *Autoriser l'utilisation d'iTunes Music Store :* si cette option est décochée, l'accès au magasin de musique en ligne iTunes Music Store est désactivé et son icône est retirée du menu principal. L'utilisateur ne peut alors pas prévisualiser, acheter ou télécharger de contenu.
- *Autoriser l'installation d'applications :* si cette option est décochée, l'accès au magasin en ligne App Store est désactivé et son icône est retirée du menu principal. L'utilisateur est en outre dans l'impossibilité d'installer ou de mettre à jour ses applications.
- *Autoriser l'utilisation de l'appareil photo :* si cette option est décochée, l'appareil photo est complètement désactivé et son icône est retirée du menu principal. L'utilisateur est alors dans l'impossibilité de prendre des photos.
- *Autoriser la capture d'écran :* lorsque cette option est désactivée, les utilisateurs sont dans l'impossibilité d'enregistrer une capture de l'écran.

Réglages Wi-Fi

Utilisez cette donnée utile pour définir la manière dont l'appareil se connecte à votre réseau sans fil. Vous pouvez ajouter plusieurs configurations réseau en cliquant sur le bouton Ajouter (+) dans la sous-fenêtre de modification.

Ces réglages doivent être spécifiés et répondre aux contraintes de votre réseau pour que l'utilisateur puisse établir une connexion.

- *SSID (Service Set Identifier) :* saisissez le SSID du réseau sans fil pour vous y connecter.
- *Réseau masqué :* spécifie si le réseau diffuse son identité.
- *Type de sécurité :* sélectionnez la méthode d'authentification du réseau. Les choix suivants sont disponibles pour les réseaux d'entreprise et privés.
  - *Aucune :* le réseau n'utilise pas d'authentification.
  - *WEP :* le réseau utilise uniquement l'authentification WEP.
  - *WPA/WPA 2 :* le réseau utilise uniquement l'authentification WPA.
  - *Quelconque :* l'appareil utilise l'authentification WEP ou WPA lorsqu'il se connecte au réseau mais ne se connectera pas aux réseaux non authentifiés.
- *Mot de passe :* saisissez le mot de passe permettant d'accéder au réseau sans fil. Si vous laissez ce champ vide, l'utilisateur doit alors saisir son mot de passe.

Réglages Entreprise

Dans cette rubrique, vous pouvez préciser des réglages de connexion à des réseaux d'entreprise. Ces réglages apparaissent si vous choisissez un réglage d'entreprise dans le menu local Type de sécurité.

Dans l'onglet Protocoles, vous pouvez spécifier les méthodes EAP qu'il faut utiliser pour l'authentification et définir les réglages relatifs au Protected Access Credential EAP-FAST.

Dans l'onglet Authentification, vous pouvez spécifier des réglages d'ouverture de session comme le nom d'utilisateur et les protocoles d'authentification. Si vous avez installé une identité par le biais de la section Références, vous pouvez sélectionner celle-ci dans le menu local Certificat d'identité.

Dans l'onglet Se fier, vous pouvez spécifier les certificats qui doivent être considérés comme dignes de confiance pour la validation du serveur d'authentification pour la connexion Wi-Fi. La liste Certificats approuvés affiche les certificats qui ont été ajoutés à l'aide de l'onglet Références et vous permet de sélectionner les certificats qui doivent être considérés comme dignes de confiance. Ajoutez les noms des serveurs d'authentification auxquels faire confiance à la liste Noms des certificats des serveurs de confiance. Vous pouvez spécifier un serveur particulier, comme *serveur.mon_entreprise.com*, ou un nom partiel, comme **.mon_entreprise.com*.

L'option Autoriser les exceptions de fiabilité permet aux utilisateurs de se fier à un serveur lorsque la chaîne de confiance ne peut pas être établie. Pour éviter ces invites et n'autoriser que les connexions aux services de confiance, désactivez cette option et incorporez tous les certificats nécessaires dans un profil.

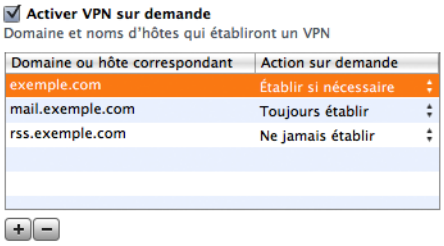
Réglages VPN

Utilisez cette donnée utile pour définir les réglages relatifs à la connexion à votre réseau. Vous pouvez ajouter plusieurs jeux de connexions en cliquant sur le bouton Ajouter (+).

Pour obtenir des informations sur les protocoles VPN et les méthodes d'authentification pris en charge, consultez « VPN » à la page 11. Les options proposées varient en fonction du protocole et de la méthode d'authentification que vous sélectionnez.

Activer VPN sur demande

Dans le cas des configurations IPSec s'appuyant sur des certificats, il vous est possible d'activer la fonction de VPN à la demande pour qu'une connexion VPN s'établisse automatiquement au moment de l'accès à certains domaines.



Les options de VPN sur demande sont :

Réglage	Description
Toujours	Établit une connexion VPN pour toute adresse correspondant au domaine indiqué.
Jamais	N'engage pas de connexion VPN pour les adresses correspondant au domaine indiqué. Si cette connexion est déjà active, elle peut néanmoins être utilisée.
Établir si nécessaire	Permet d'établir une connexion VPN pour les adresses correspondant au domaine indiqué uniquement après un échec de recherche de DNS.

L'action s'applique à toutes les adresses correspondantes. Les adresses sont comparées par correspondance de simple chaîne, en commençant par la fin et en revenant en arrière. L'adresse « .example.org » s'apparente à « support.example.org » et à « sales.example.org » mais pas à « www.private-example.org ». Néanmoins, si vous spécifiez le domaine de correspondance « example.com » (notez l'absence de point au début), il s'apparente à « www.private-example.com » et à tous les autres.

N'oubliez pas que les connexions LDAP n'établissent pas de connexion VPN ; si celle-ci n'a pas été établie par une autre application, telle que Safari, la recherche LDAP échoue.

Proxy VPN

L'iPhone prend en charge la configuration d'un proxy VPN manuelle et la configuration automatique d'un proxy à travers PAC ou WPAD. Pour indiquer un proxy VPN, sélectionnez une option dans le menu local Configuration du proxy.

Dans le cas des configurations PAC de proxy automatique, sélectionnez Automatique dans le menu local puis tapez l'URL d'un fichier PAC. Pour en savoir plus sur les fonctionnalités PACS et sur le format de fichier, consultez « Autres ressources » à la page 60.

En ce qui concerne les configurations WPAD (Web Proxy Autodiscovery) , sélectionnez Automatique dans le menu local. Laissez le champ « URL du serveur proxy » vide ; l'iPhone demande alors le fichier WPAD par le biais des protocoles DHCP et DNS. Pour en savoir plus sur le WPAD, consultez « Autres ressources » à la page 60

Réglages du courrier électronique

Utilisez cette donnée utile pour configurer les comptes de messagerie POP ou IMAP de l'utilisateur. Si vous ajoutez un compte Exchange, consultez les réglages Exchange ci-dessous.

Les utilisateurs peuvent modifier certains des réglages relatifs au courrier électronique que vous fournissez dans un profil, comme le nom du compte, le mot de passe et les serveurs SMTP alternatifs. Si vous omettez l'une ou l'autre de ces informations dans le profil, les utilisateurs sont alors invités à la saisir lorsqu'ils accèdent au compte.

Vous pouvez ajouter plusieurs comptes de courrier électronique en cliquant sur le bouton Ajouter (+).

Réglages Exchange

Utilisez cette donnée utile pour saisir les réglages utilisateur de votre serveur Exchange. Vous pouvez créer un profil pour un utilisateur spécifique en précisant le nom d'utilisateur, le nom d'hôte et l'adresse électronique, ou ne fournir que le nom d'hôte. Dans ce dernier cas, les utilisateurs sont alors invités à fournir les valeurs manquantes lorsqu'ils installent le profil.

Si vous spécifiez le nom d'utilisateur, le nom d'hôte et le réglage SSL dans le profil, l'utilisateur ne peut pas modifier ces réglages sur l'appareil.

Vous ne pouvez configurer qu'un compte Exchange par appareil. Les autres comptes de messagerie, comme les comptes IMAP Exchange, ne sont pas affectés lorsque vous ajoutez un compte Exchange. Les comptes Exchange qui sont ajoutés par le biais d'un profil sont supprimés si le profil l'est également, et ne peuvent pas l'être d'une autre façon.

Par défaut, Exchange synchronise les contacts, les calendriers et le courrier électronique. L'utilisateur peut modifier ces réglages sur l'appareil, notamment le nombre de jours de données à synchroniser, dans Réglages > Comptes.

Si vous sélectionnez l'option Utiliser SSL, n'oubliez pas d'ajouter les certificats nécessaires pour authentifier la connexion à l'aide de la sous-fenêtre Références.

Pour fournir un certificat identifiant l'utilisateur auprès du serveur Exchange ActiveSync, cliquez sur le bouton Ajouter (+) puis sélectionnez un certificat d'identité dans le trousseau de Mac OS X ou dans le magasin de certificats de Windows. Après avoir ajouté un certificat, vous pouvez spécifier le nom d'authentification, s'il est nécessaire à votre configuration ActiveSync. Vous pouvez également intégrer la phrase clé du certificat dans le profil de configuration. Si vous ne fournissez pas la phrase clé, l'utilisateur est invité à la saisir lorsque le profil est installé.

Réglages LDAP

Utilisez cette donnée utile pour définir les réglages permettant d'établir une connexion à un annuaire LDAPv3. Vous pouvez indiquer plusieurs bases de recherche pour chaque annuaire et configurer plusieurs connexions à des annuaires en cliquant sur le bouton Ajouter (+).

Si vous sélectionnez l'option Utiliser SSL, n'oubliez pas d'ajouter les certificats nécessaires pour authentifier la connexion à l'aide de la sous-fenêtre Références.

Réglages CalDAV

Utilisez cette donnée utile pour fournir les réglages des comptes pour la connexion à un serveur de calendrier compatible CalDAV. Ces comptes seront ajoutés à l'appareil et, comme pour les comptes Exchange, les utilisateurs devront saisir manuellement les informations que vous avez omises dans le profil, comme le mot de passe de leur compte, à l'installation du profil.

Si vous sélectionnez l'option Utiliser SSL, n'oubliez pas d'ajouter les certificats nécessaires pour authentifier la connexion à l'aide de la sous-fenêtre Références.

Vous pouvez configurer plusieurs comptes en cliquant sur le bouton Ajouter (+).

Réglages « Calendriers auxquels vous êtes abonné »

Utilisez cette donnée utile pour ajouter des abonnements à des calendriers en lecture seule à application Calendrier de l'appareil. Vous pouvez configurer plusieurs abonnements en cliquant sur le bouton Ajouter (+).

La liste des calendriers publics auxquels il vous est possible de vous abonner est disponible à l'adresse www.apple.com/downloads/macosx/calendars/ (en anglais).

Si vous sélectionnez l'option Utiliser SSL, n'oubliez pas d'ajouter les certificats nécessaires pour authentifier la connexion à l'aide de la sous-fenêtre Références.

Réglages Clip web

Utilisez cette donnée utile pour ajouter des clips web au menu principal de l'appareil de l'utilisateur. Les clips web assurent un accès rapide aux pages web favorites.

Assurez-vous que l'URL que vous saisissez reprend le préfixe http:// ou https://, lequel est obligatoire pour que le clip web fonctionne. Par exemple, pour ajouter à l'écran d'accueil la version en ligne du *« Guide de l'utilisateur iPhone »*, spécifiez l'URL du clip web : http://help.apple.com/iphone/

Pour ajouter une icône personnalisée, sélectionnez un graphique au format gif, jpeg ou png, de dimensions 59 x 60 pixels. L'image est automatiquement mise à l'échelle, rognée et convertie au format png, si nécessaire.

Réglages de références

Utilisez cette donnée utile pour ajouter des certificats et des identités à l'appareil. Pour en savoir plus sur les formats pris en charge, consultez « Certificats et identités » à la page 12.

Lorsque vous installez des références, installez également les certificats intermédiaires nécessaires pour établir une chaîne vers un certificat approuvé se trouvant sur l'appareil. Pour afficher une liste des racines préinstallées, consultez l'article de l'assistance Apple à l'adresse http://support.apple.com/kb/HT2185 (en anglais uniquement).

Si vous ajoutez un identifiant à utliser avec Microsoft Exchange, utilisez plutôt les données Exchange. Consultez « Réglages Exchange » à la page 39.

Ajout de références sur Mac OS X :

1. Cliquez sur le bouton Ajouter (+).
2. Dans la zone de dialogue qui apparaît pour le fichier, sélectionnez un fichier PKCS1 ou PKSC12, puis cliquez sur Ouvrir.

   Si le certificat ou l'identité à installer dans votre trousseau, passez par Trousseau d'accès pour l'exporter au format .p12. Trousseau d'accès se trouve dans le dossier /Applications/Utilitaires. Pour obtenir de l'aide, consultez l'Aide de Trousseau d'accès, accessible depuis le menu Aide lorsque le programme Trousseau d'accès est ouvert.

   Pour ajouter plusieurs références au profil de configuration, recliquez sur le bouton Ajouter (+).

Ajout de références sur Windows :

1. Cliquez sur le bouton Ajouter (+).
2. Sélectionnez la référence à installer depuis le magasin de certificats de Windows.

   Si celle-ci n'est pas proposée dans votre magasin de certificats personnel, vous devez l'y ajouter et marquer la clé privée comme exportable, ce qui constitue d'ailleurs l'une des étapes qu'offre l'Assistant Importation de certificats. Il est important de noter que l'ajout d'un certificat racine requiert un accès administrateur à l'ordinateur, et vous devez ajouter le certificat à votre magasin personnel.

   Si vous utilisez plusieurs profils de configuration, assurez-vous que les certificats ne sont pas en double. Vous ne pouvez pas installer plusieurs copies d'un même certificat.

   Au lieu d'installer des certificats à l'aide d'un profil de configuration, vous pouvez autoriser aux utilisateurs d'utiliser Safari pour télécharger les certificats directement sur leur appareil à partir d'une page web. Vous pouvez également envoyer les certificats aux utilisateurs par courrier électronique. Consultez « Installation d'identités et de certificats racine » à la page 59 pour en savoir plus. Vous pouvez aussi passer par les réglages SCEP situés en dessous pour préciser le mode de récupération des certificats par l'appareil activé en mode OTA, une fois le profil installé.

Réglages SCEP

La donnée utile SCEP vous permet de préciser les réglages chargés d'autoriser l'appareil à obtenir des certificats auprès d'un AC par le biais du protocole SCEP (Simple Certificate Enrollment Protocol).

Réglage	Description
URL	Cette valeur constitue l'adresse du serveur SCEP.
Name	Cette valeur peut prendre la forme de n'importe quelle chaîne compréhensible par l'autorité de certificat. Elle permet entre autres de distinguer entre différentes instances.
Subject	Représentation d'un nom X.500 par un tableau de valeurs OID-valeur. Par exemple, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, qui peut se traduire de la manière suivante : [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]]
Challenge	Secret prépartagé que le serveur SCEP peut exploiter pour identifier la demande ou l'utilisateur.
Key Size and Usage	Sélectionnez une taille de clé et, à l'aide des cases situées sous ce champ, l'usage considéré comme acceptable de la clé.
Fingerprint	Si votre autorité de certificat utilise HTTP, utilisez ce champ pendant le processus d'inscription pour fournir l'empreinte du certificat de l'autorité que l'appareil utilisera pour confirmer l'authenticité de la réponse à l'autorité de certificat. Vous pouvez saisir une empreinte SHA1 ou MD5 ou sélectionner un certificat pour importer sa signature.

Pour en savoir plus sur la manière qu'utilise l'iPhone pour obtenir sans fil des certificats, consultez « Inscription et configuration en mode OTA » à la page 24

Réglages avancés

La donnée utile Avancé vous permet de modifier les réglages relatifs au nom du point d'accès (en anglais « Access Point Name » ou « APN ») et ceux portant sur les proxys de réseau cellulaire de l'appareil. Ces réglages définissent la manière dont l'appareil se connecte au réseau d'un opérateur de télécommunication. Ne modifiez ces réglages que si vous y êtes invité par un expert réseau de l'opérateur. Si ces réglages sont incorrects, l'appareil ne peut pas accéder aux données à l'aide du réseau de téléphonie cellulaire. Pour annuler une modification apportée à ces réglages par inadvertance, supprimez le profil de l'appareil. Apple recommande que vous définissiez les réglages APN dans un profil de configuration séparé des autres réglages d'entreprise, car les profils qui spécifient des informations doivent être signés par votre fournisseur de services mobiles.

L'iPhone OS prend en charge les noms d'utilisateurs APN pouvant s'étendre jusqu'à 20 caractères et les mots de passe de 32 caractères.

Modification de profils de configuration

Dans « Utilitaire de configuration iPhone », sélectionnez un profil dans la liste Profils de configuration, puis faites appel à la liste des données utiles et les sous-fenêtres de réglages pour y apporter des modifications. Vous pouvez également importer un profil en choisissant Fichier > Ajouter à la bibliothèque, puis en sélectionnant un fichier .mobileconfig. Si les sous-fenêtres de réglages ne sont pas visibles, choisissez Présentation > Afficher les détails.

Le champ Identifiant de la donnée utile Général est utilisé par l'appareil pour déterminer si un profil est nouveau ou s'il s'agit d'une mise à jour d'un profil existant. Si vous voulez remplacer un profil que des utilisateurs ont déjà installé par le profil mis à jour, ne changez pas l'identifiant.

Installation de profils d'approvisionnement et d'applications

« Utilitaire de configuration iPhone » peut installer des applications et des profils d'approvisionnement à la distribution sur des dispositifs connectés à l'ordinateur sur lequel l'utilitaire est installé. Pour en savoir plus, consultez le chapitre 5, « Déploiement d'applications, » à la page 69.

Installation de profils de configuration

Après avoir créé un profil, vous avez la possibilité de brancher un appareil et d'y installer le profil par le biais d'« Utilitaire de configuration iPhone ».

Une autre solution consiste à distribuer le profil aux utilisateurs par courrier électronique ou en le publiant sur un site web. Si des utilisateurs ouvrent un message électronique ou téléchargent le profil à partir du web à travers leur appareil, ils sont alors invités à lancer le processus d'installation.

Installation de profils de configuration à l'aide d'« Utilitaire de configuration iPhone »

Vous pouvez installer des profils de configuration directement sur un appareil ayant été mis à jour au système d'exploitation iPhone OS 3.0 ou ultérieur, et étant branché sur votre ordinateur. Vous pouvez aussi passer par « Utilitaire de configuration iPhone » pour supprimer des profils installés.

Pour installer un profil de configuration :

1. Branchez l'appareil sur votre ordinateur à l'aide d'un câble USB.

   Après un court instant, l'appareil apparaît dans « Utilitaire de configuration iPhone », dans la liste Appareils.
2. Sélectionnez le dispositif, puis cliquez sur l'onglet Profils de configuration.
3. Sélectionnez un profil de configuration dans la liste, puis cliquez sur Installer.

4 Sur l'appareil, sélectionnez Installer pour installer le profil.

Si vous installez directement sur un équipement à travers un branchement USB, le profil de configuration est automatiquement signé et chiffré avant son transfert à l'appareil.

Distribution de profils de configuration par courrier électronique

Vous pouvez distribuer les profils de configuration par courrier électronique. Les utilisateurs installent le profil en ouvrant le message reçu sur leur appareil, puis en indiquant la pièce jointe à installer.

Pour envoyer par courrier électronique un profil de configuration :

1 Dans « Utilitaire de configuration iPhone », sur la barre d'outils, cliquez sur le bouton Partager.

Dans la zone de dialogue qui s'affiche, sélectionnez une option de sécurité :

a *Aucune :* un fichier .mobileconfig au format Texte est alors créé. Celui-ci peut s'installer sur n'importe quel appareil. Certaines parties du contenu du fichier sont brouillées afin d'empêcher tout regard « par dessus l'épaule » en cas de consultation du fichier.

b *Signer le profil de configuration :* le fichier .mobileconfig est signé et ne peut pas s'installer sur un appareil s'il a été modifié. Certains champs sont brouillés afin d'empêcher tout regard « par dessus l'épaule » en cas de consultation du fichier. Une fois installé, un autre profil ne peut mettre à jour ce profil que si le premier possède le même identifiant et est signé par la même copie d'« Utilitaire de configuration iPhone ».

c *Signer le profil de configuration/Chiffrer le profil :* la première option permet de signer le profil afin qu'il ne puisse pas être modifié, et la seconde chiffre l'intégralité du contenu de sorte que personne d'autre ne peut examiner le profil et que le profil ne peut s'installer que sur un appareil donné. Si le profil contient des mots de passe, cette option est recommandée. Un fichier .mobileconfig est créé pour chacun des appareils sélectionnés dans la liste Appareils. Si un dispositif n'apparaît pas dans la liste, soit il se peut qu'il n'a jamais été branché sur l'ordinateur pour récupérer la clé de chiffrement, soit il se peut qu'il n'a pas été mis à niveau au système d'exploitation pour portable iPhone OS 3.0 ou ultérieur.

2 Cliquez sur Partager. Un nouveau message Mail (Mac OS X) ou Outlook (Windows) s'ouvre alors avec les profils en pièces jointes sans compression. Les fichiers doivent être sans compression pour que l'appareil reconnaisse et installe le profil.

Distribution de profils de configuration sur le web

Vous pouvez distribuer les profils de configuration par le biais d'un site web. Les utilisateurs peuvent installer le profil en le téléchargeant sur leur appareil par le biais de Safari. Pour distribuer facilement l'URL à vos utilisateurs, envoyez-le par SMS.

Pour exporter un profil de configuration :

1. Dans « Utilitaire de configuration iPhone », sur la barre d'outils, cliquez sur le bouton Exporter.

   Dans la zone de dialogue qui s'affiche, sélectionnez une option de sécurité :

   a. *Aucune :* un fichier .mobileconfig au format Texte est alors créé. Celui-ci peut s'installer sur n'importe quel appareil. Certaines parties du contenu du fichier sont brouillées afin d'empêcher tout regard « par dessus l'épaule » en cas de consultation du fichier, mais vous devez vous assurer, lorsque vous placez le fichier sur votre site web, qu'il n'est accessible que par des utilisateurs autorisés.

   b. *Signer le profil de configuration :* le fichier .mobileconfig est signé et ne peut pas s'installer sur un appareil s'il a été modifié. Une fois installé, un autre profil ne peut mettre à jour ce profil que si le premier possède le même identifiant et est signé par la même copie d'« Utilitaire de configuration iPhone ». Certaines informations du profil sont brouillées afin d'empêcher tout regard « par dessus l'épaule » en cas de consultation du fichier, mais vous devez vous assurer, lorsque vous placez le fichier sur votre site web, qu'il n'est accessible que par des utilisateurs autorisés.

   c. *Signer le profil de configuration/Chiffrer le profil :* la première option permet de signer le profil afin qu'il ne puisse pas être modifié, et la seconde chiffre l'intégralité du contenu de sorte que personne d'autre ne peut examiner le profil et que le profil ne peut s'installer que sur un appareil donné. Un fichier .mobileconfig est créé pour chacun des appareils sélectionnés dans la liste Appareils.

2. Cliquez sur Exporter, puis sélectionnez un emplacement où enregistrer les fichiers .mobileconfig.

   Les fichiers sont prêts à être publiés sur votre site web. Ne compressez pas le fichier .mobileconfig et ne modifiez pas son extension, sinon l'appareil ne reconnaîtra pas ou n'installera pas le profil.

Installation par les utilisateurs de profils de configuration téléchargés

Fournissez à vos utilisateurs l'URL à laquelle ils peuvent télécharger les profils sur leur appareil ou envoyez ces profils à un compte de messagerie auquel vos utilisateurs ont accès par le biais de leur appareil avant d'y ajouter les informations propres à votre entreprise.

Si un utilisateur télécharge le profil du web ou ouvre la pièce jointe dans Courrier, l'appareil reconnaît alors le profil sous la forme de l'extension .mobileconfig et lance l'installation si l'utilisateur sélectionne Installer.

Pendant l'installation, les utilisateurs sont invités à saisir toutes les informations nécessaires, comme les mots de passe qui n'auront pas été indiqués dans le profil, ainsi que d'autres informations demandées par les réglages que vous avez précisés.

L'appareil extrait également les règlements Exchange ActiveSync du serveur et les actualise si elles ont été modifiées, à chaque nouvelle connexion. Si l'appareil ou les règlements Exchange ActiveSync rendent obligatoire un réglage de code, l'utilisateur doit saisir un code conforme au règlement pour pouvoir terminer l'installation.

L'utilisateur est en outre invité à saisir tous les mots de passe nécessaires pour pouvoir utiliser les certificats qui figurent dans le profil.

Si l'installation ne se termine pas correctement, par exemple, si le serveur Exchange est injoignable ou si l'utilisateur a annulé l'opération, aucune des informations saisies par l'utilisateur n'est conservée.

Les utilisateurs peuvent modifier la durée en jours de conservation des messages lors d'une synchronisation sur l'appareil et indiquer les dossiers de messagerie électronique à synchroniser, en plus de la boîte de réception. Les valeurs respectives par défaut sont de trois jours et tous les dossiers. Vous pouvez les changer en accédant à Réglages > Courrier, Contacts, Calendrier > *nom du compte Exchange*.

Suppression et mise à jour de profils de configuration

Les mises à jour des profils de configuration ne sont pas transmises automatiquement aux utilisateurs. Distribuez les profils à jour à vos utilisateurs pour que ceux-ci les installent. À condition que l'identifiant de configuration du profil correspond, et s'il est signé, que la même copie d'« Utilitaire de configuration iPhone » l'a signé, le nouveau profil remplace celui qui se trouve sur l'appareil.

Les réglages rendus obligatoires par un profil de configuration ne peuvent pas être modifiés sur l'appareil. Pour modifier un réglage, vous devez installer un profil actualisé. Si le profil a été signé, il ne peut alors être remplacé que par un autre signé par la même copie d'« Utilitaire de configuration iPhone ». Les identifiants des deux profils doivent coïncider afin que le profil à jour soit reconnu en tant que profil de remplacement. Pour en savoir plus sur l'identifiant, consultez « Réglages généraux » à la page 34.

Important : la suppression d'un profil de configuration entraîne celle des règlements et de toutes les données du compte Exchange stockées sur l'appareil, de même que les réglages VPN, les certificats et les autres informations, y compris les courriers électroniques, associées au profil.

Configuration manuelle d'appareils

3

Le présent chapitre décrit comment configurer l'iPhone, l'iPod touch et l'iPad manuellement.

Si vous ne fournissez pas de profils de configuration automatique, les utilisateurs peuvent configurer leurs appareils manuellement. Certains réglages, comme les règlements de code, ne peuvent être définis qu'à l'aide d'un profil de configuration.

Réglages VPN

Pour modifier des réglages VPN, allez à Réglages > Général > Réseau > VPN.

Lorsque vous configurez des réglages VPN, l'appareil vous invite à saisir des informations en fonction des réponses qu'il reçoit de votre serveur VPN. Par exemple, il vous invite à saisir un jeton SecurID RSA si le serveur en exige un.

Vous ne pouvez pas configurer une connexion VPN à base de certificats si les certificats appropriés ne sont pas installés sur l'appareil. Consultez « Installation d'identités et de certificats racine » à la page 59 pour en savoir plus.

Le VPN sur demande ne peut pas être configuré sur l'appareil, vous devez dans ce cas le définir par le biais d'un profil de configuration. Reportez-vous à la section « Activer VPN sur demande » à la page 38.

Réglages Proxy VPN

Il vous est également possible, pour toutes les configurations, d'indiquer un proxy VPN. Pour configurer un seul proxy pour toutes les connexions, sélectionnez Manuel et indiquez l'adresse, le port et, le cas échéant, les données d'authentification. Pour enrichir l'appareil d'un fichier de configuration de proxy automatique, sélectionnez Auto puis indiquez l'URL du fichier PACS. Pour spécifier la configuration de proxy automatique à l'aide du protocole WPAD, sélectionnez Automatique. L'appareil lancera des requêtes DHCP et DNS pour obtenir les réglages WPAD. Consultez les exemples de fichiers PACS et autres ressources à la fin de ce chapitre, dans la rubrique Autres ressources.

Réglages Cisco IPSec

Lorsque vous configurez l'appareil manuellement pour un VPN Cisco IPSec, un écran de ce type apparaît :

Utilisez ce tableau pour identifier les réglages et les informations à saisir :

Champ	Description
Description	Titre descriptif qui identifie ce groupe de réglages.
Serveur	Nom DNS ou adresse IP du serveur VPN auquel il faut se connecter.
Compte	Nom de l'utilisateur du compte de session VPN de l'utilisateur. Ne saisissez pas le nom du groupe dans ce champ.
Mot de passe	La phrase clé du compte d'ouverture de session VPN de l'utilisateur. Laissez le champ vide pour l'authentification RSA SecurID et CryptoCard ou si vous voulez que les utilisateurs saisissent leur mot de passe manuellement à chaque tentative de connexion.
Utiliser le certificat	N'est disponible que si vous avez installé une identité .p12 ou .pfx contenant un certificat permettant l'accès à distance *et* la clé privée du certificat. Lorsque Utiliser le certificat est activé, les champs Nom du groupe et Secret partagé sont remplacés par un champ Identifier qui vous permet de faire votre choix dans la liste des identités compatibles VPN installées.
Nom du groupe	Nom du groupe auquel l'utilisateur appartient tel que défini sur le serveur VPN.
Secret	Secret partagé du groupe. Identique pour chaque membre du groupe assigné à l'utilisateur. Il ne s'agit *pas* du mot de passe de l'utilisateur et il doit être spécifié pour établir une connexion.

Réglages PPTP

Lorsque vous configurez l'appareil manuellement pour un VPN PPTP, un écran semblable à l'écran suivant apparaît :

Utilisez ce tableau pour identifier les réglages et les informations à saisir :

Champ	Description
Description	Titre descriptif qui identifie ce groupe de réglages.
Serveur	Nom DNS ou adresse IP du serveur VPN auquel il faut se connecter.
Compte	Nom de l'utilisateur du compte de session VPN de l'utilisateur.
RSA SecurID	Si vous utilisez un jeton RSA SecurID, activez cette option afin que le champ Mot de passe soit masqué.
Mot de passe	La phrase clé du compte d'ouverture de session VPN de l'utilisateur.
Niveau de chiffrement	Auto est la valeur par défaut et sélectionne le degré de chiffrement le plus élevé disponible, en commençant par 128 bits, puis 40 bits, puis Aucun. Le maximum est 128 bits uniquement. Aucun désactive le chiffrement.
Tout envoyer	La valeur par défaut correspond à Oui. Envoie tout le trafic réseau par le lien VPN. Désactivez cette option pour activer le split-tunneling, qui route uniquement le trafic destiné aux serveurs qui se trouvent sur le réseau VPN par le serveur. Le reste du trafic est routé directement vers Internet.

Réglages L2TP

Lorsque vous configurez l'appareil manuellement pour un VPN L2TP, un écran semblable à l'écran suivant apparaît :

Utilisez ce tableau pour identifier les réglages et les informations à saisir :

Champ	Description
Description	Titre descriptif qui identifie ce groupe de réglages.
Serveur	Nom DNS ou adresse IP du serveur VPN auquel il faut se connecter.
Compte	Nom de l'utilisateur du compte de session VPN de l'utilisateur.
Mot de passe	Mot de passe du compte de session VPN de l'utilisateur.
Secret	Secret partagé (clé prépartagée) du compte L2TP. Identique pour tous les utilisateurs LT2P.
Tout envoyer	La valeur par défaut correspond à Oui. Envoie tout le trafic réseau par le lien VPN. Désactivez cette option pour activer le split-tunneling, qui route uniquement le trafic destiné aux serveurs qui se trouvent sur le réseau VPN par le serveur. Le reste du trafic est routé directement vers Internet.

Réglages Wi-Fi

Pour modifier des réglages Wi-Fi, allez à Réglages > Général > Réseau > Wi-Fi. Si le réseau que vous ajoutez est à portée, sélectionnez-le dans la liste des réseaux disponibles. À défaut, touchez Autre.

Assurez-vous que votre infrastructure réseau utilise une authentification et un chiffrement pris en charge par l'iPhone et l'iPod touch. Pour obtenir des spécifications, consultez « Sécurité réseau » à la page 12. Pour en savoir plus sur l'installation de certificats pour l'authentification, consultez« Installation d'identités et de certificats racine » à la page 59.

Réglages Exchange

Vous ne pouvez configurer qu'un compte Exchange par appareil. Pour ajouter un compte Exchange, allez à Réglages > Mail, Contacts, Calendrier puis touchez Ajouter un compte. À l'écran Ajouter un compte, touchez Microsoft Exchange.

Lorsque vous configurez manuellement l'appareil pour Exchange, utilisez le tableau qui suit pour identifier les réglages et les informations à saisir :

Champ	Description
Adresse	Adresse électronique complète de l'utilisateur.
Domaine	Domaine du compte Exchange de l'utilisateur.
Nom d'utilisateur	Nom de l'utilisateur du compte Exchange.
Mot de passe	Mot de passe du compte Exchange de l'utilisateur.
Description	Titre descriptif qui identifie ce compte.

L'iPhone, l'iPod touch et l'iPad prennent en charge le service de découverte automatique de Microsoft, qui utilise votre nom d'utilisateur et votre mot de passe pour déterminer l'adresse du serveur Exchange frontal. Si l'adresse du serveur ne peut pas être déterminée, vous serez invité à la saisir.

Si votre serveur Exchange écoute les connexions sur un autre port que le 443, indiquez ce port dans le champ Serveur sous la forme *exchange.example.com:portnumber*.

Une fois que le compte Exchange est configuré, les règlements de code du serveur sont appliqués. Si le code en vigueur de l'utilisateur n'est pas conforme aux règlements Exchange ActiveSync, l'utilisateur est invité à modifier ou à définir le code. L'appareil ne communique alors pas avec le serveur Exchange tant que l'utilisateur n'a pas défini de code conforme aux règlements Exchange ActiveSync.

Ensuite, l'appareil propose de se synchroniser immédiatement avec le serveur Exchange. Si vous choisissez de ne pas synchroniser les données à ce moment, vous pouvez activer ultérieurement la synchronisation des calendriers et des contacts dans Réglages > Mail, Contacts, Calendrier. Par défaut, Exchange ActiveSync transmet les nouvelles données à votre appareil au fur et à mesure qu'elles arrivent sur le serveur (« push »). Si vous préférez rechercher les nouvelles données selon un programme ou ne rechercher les nouvelles données que manuellement, utilisez Réglages > Mail, Calendrier > Nouvelles données pour modifier les réglages.

Pour modifier le nombre de jours correspondant aux messages électroniques à synchroniser sur votre appareil, accédez à Réglages > Mail, Contacts, Calendrier, puis sélectionnez le compte Exchange. Vous pouvez également sélectionner les dossiers, en plus de celui de la boîte de réception, à inclure dans la remise push du courrier électronique.

Pour changer de réglage pour les données de calendrier, accédez à Réglages > Mail, Contacts, Calendriers > Synchroniser.

Réglages LDAP

L'iPhone, l'iPod touch et l'iPad peuvent rechercher les données de contacts situées sur des serveurs d'annuaire LDAP. Pour ajouter un serveur LDAP, accédez à Réglages > Mail, Contacts, Calendrier > Ajouter un compte > Autre. Sélectionnez ensuite « Ajouter un compte LDAP ».

Saisissez l'adresse du serveur LDAP, ainsi que le nom d'utilisateur et le mot de passe si nécessaire, puis sélectionnez Suivant. Si le serveur est accessible et fournit les réglages de recherche par défaut à l'appareil, ceux-ci sont alors utilisés.

Les réglages « Étendue de la recherche » suivants sont pris en charge :

Réglage « Étendue de la recherche »	Description
Base	Recherche uniquement l'objet de base.
Un niveau	Recherche les objets immédiatement inférieurs à l'objet de base, sans inclure l'objet de base même.
Sous-arbre	Recherche l'objet de base et l'intégralité de son arborescence où se trouvent tous les objets qui en descendent.

Vous avez la possibilité de définir plusieurs ensembles de réglages de recherche pour chaque serveur.

Réglages CalDAV

L'iPhone, l'iPod touch et l'iPad fonctionnent avec les serveurs de calendrier CalDAV qui fournissent les calendriers de groupe et les programmations. Pour ajouter un serveur CalDAV, accédez à Réglages > Mail, Contacts, Calendrier > Ajouter un compte > Autre. Sélectionnez ensuite « Ajouter un compte CalDAV ».

Saisissez l'adresse du serveur CalDAV, ainsi que le nom d'utilisateur et le mot de passe si nécessaire, puis sélectionnez Suivant. Après la prise de contact avec le serveur, les autres champs apparaissent pour vous permettre de définir des options supplémentaires.

Réglages Abonnement à un calendrier

Vous pouvez ajouter des calendriers en lecture seule, tels que ceux prévoyant les programmations de projet ou les vacances. Pour ajouter un calendrier, accédez à Réglages > Mail, Contacts, Calendrier > Ajouter un compte > Autre, puis Ajouter un calendrier (abonnement).

Saisissez l'URL d'un fichier iCalendar (.ics), ainsi que le nom et le mot de passe de l'utilisateur si nécessaire, puis sélectionnez Enregistrer. Vous avez également la possibilité de préciser si les alarmes définies dans le calendrier doivent être supprimées lorsque ce dernier est ajouté à l'appareil.

En plus de l'ajout manuel d'abonnements à des calendriers, vous pouvez envoyer aux utilisateurs un URL webcal:// (ou un lien HTTP:// vers un fichier .ics) et, après que l'utilisateur ait sélectionné le lien, l'appareil propose d'ajouter l'URL aux calendriers abonnés.

Installation d'identités et de certificats racine

Si vous ne distribuez pas de certificats à l'aide de profils, vos utilisateurs peuvent les installer manuellement en utilisant l'appareil pour les télécharger d'un site web ou en ouvrant une pièce jointe dans un message électronique. L'appareil reconnaît les certificats avec les types MIME et les extensions de fichier suivants :

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

Pour en savoir plus sur les formats et autres configurations requises, consultez « Certificats et identités » à la page 12.

Une fois qu'un certificat ou une identité est téléchargé sur l'appareil, l'écran Installer le profil apparaît. La description est du type :identité ou autorité de certificat. Pour installer le certificat, touchez Installer. S'il correspond à un certificat d'identité, vous êtes alors invité à saisir le mot de passe du certificat.

Pour afficher ou supprimer un certificat installé, accédez à Réglages > Général > Profil. Si vous supprimez un certificat nécessaire pour accéder à un compte ou à un réseau, votre appareil ne peut alors pas se connecter à ces services.

Comptes de courrier électronique supplémentaires

Bien que vous ne puissiez configurer qu'un seul compte Exchange, vous pouvez ajouter plusieurs comptes POP et IMAP. Cela permet, par exemple, d'accéder à du courrier électronique sur un serveur de messagerie Lotus Notes ou Novell Groupwise. Accédez à Réglages > Comptes > Mail, Contacts, Calendrier > Ajouter un compte > Autre. Pour en savoir plus sur l'ajout d'un compte IMAP, consultez le *Guide de l'utilisateur de l'iPhone, le Guide de l'utilisateur de l'iPod touch* ou *le Guide de l'utilisateur de l'iPad*.

Mise à jour et suppression de profils

Pour savoir comment l'utilisateur peut mettre à jour ou supprimer des profils de configuration, consultez « Suppression et mise à jour de profils de configuration » à la page 48.

Pour en savoir plus sur l'installation de profils d'approvisionnement à la distribution, consultez « Déploiement d'applications » à la page 69.

Autres ressources

Pour en savoir plus sur le format et la fonction des fichiers de configuration de proxy automatique employés par les réglages Proxy VPN, reportez-vous à ce qui suit :

- article en anglais sur la technologie PAC (Proxy auto-config), à l'adresse http://en.wikipedia.org/wiki/Proxy_auto-config ;
- article en anglais sur le protocole Web Proxy Autodiscovery Protocol, à l'adresse http://en.wikipedia.org/wiki/Wpad ;
- article en anglais Microsoft TechNet « Using Automatic Configuration, Automatic Proxy, and Automatic Detection » (Utilisation de la configuration automatique, de proxy automatique et de la détection automatique) à l'adresse http://technet.microsoft.com/fr-fr/library/dd361918(en-us).aspx ;

Apple dispose de plusieurs didacticiels visionnables dans un navigateur web standard qui montrent à vos utilisateurs comment configurer et utiliser les fonctionnalités de l'iPhone, de l'iPod touch et de l'iPad :

- visite guidée de l'iPhone, à l'adresse http://www.apple.com/fr/iphone/guidedtour/ ;
- visite guidée de l'iPod touch, à l'adresse www.apple.com/fr/ipodtouch/guidedtour/ ;
- visite guidée de l'iPad, à l'adresse www.apple.com/ipad/guided-tours/ ;
- page web d'assistance pour l'iPhone, à l'adresse www.apple.com/fr/support/iphone/ ;
- page web d'assistance pour l'iPod touch, à l'adresse www.apple.com/fr/support/ipodtouch/.
- page web d'assistance pour l'iPad, à l'adresse www.apple.com/fr/support/ipad/ ;

Il existe également un guide de l'utilisateur pour chaque appareil, au format PDF, qui contient des astuces et des détails d'utilisation supplémentaires :

- *Guide de l'utilisateur de l'iPhone :*
  http://manuals.info.apple.com/fr_FR/iPhone_Guide_de_l_utilisateur.pdf
- *Guide de l'utilisateur de l'iPod touch :*
  http://manuals.info.apple.com/fr_FR/iPod_touch_3.0_Guide_de_l_utilisateur.pdf
- *Guide de l'utilisateur de l'iPad :*
  http://manuals.info.apple.com/fr/iPad_Guide_de_l_utilisateur.pdf

Déploiement d'iTunes

4

L'on utilise iTunes pour synchroniser de la musique et de la vidéo, installer des applications, et bien plus encore.

Le présent chapitre décrit comment déployer iTunes et des applications d'entreprise, et définit les réglages et les restrictions que vous pouvez spécifier.

L'iPhone, l'iPod touch et l'iPad peuvent synchroniser chaque type de données (musique, données multimédia, etc.) avec un seul ordinateur à la fois. Par exemple, vous avez la possibilité de synchroniser de la musique avec un ordinateur de bureau et les signets avec un ordinateur portable, en définissant de façon appropriée les options de synchronisation d'iTunes sur les deux ordinateurs. Consultez l'Aide d'iTunes accessible depuis le menu Aide, pour en savoir plus sur les options de synchronisation.

Installation d'iTunes

iTunes utilise les programmes d'installation standard Macintosh et Windows. La dernière version et la liste de la configuration requise sont proposées au téléchargement à l'adresse www.itunes.com/fr.

Pour en savoir plus sur les exigences en matière de licence pour la distribution d'iTunes, reportez-vous à :
http://developer.apple.com/softwarelicensing/agreements/itunes.html (en anglais).

Installation d'iTunes sur des ordinateurs Windows

Lorsque vous installez iTunes sur des ordinateurs Windows, par défaut vous installez également la dernière version de QuickTime, Bonjour et d'Apple Software Update. Vous pouvez omettre ces composants en passant des paramètres au programme d'installation d'iTunes en ne transmettant par push que les composants que vous voulez installer sur les ordinateurs des utilisateurs dont vous avez la charge.

Installation sous Windows à l'aide d'iTunesSetup.exe

Si vous pensez utiliser le processus d'installation standard d'iTunes, en omettant certains composants, vous pouvez passer des propriétés vers iTunesSetup.exe en utilisant la ligne de commande.

Propriété	Signification
NO_AMDS=1	Ne pas installer Apple Mobile Device Services. Ce composant est obligatoire pour qu'iTunes puisse synchroniser et gérer des appareils mobiles.
NO_ASUW=1	Ne pas installer Apple Software Update pour Windows. Cette application alerte les utilisateurs lorsque de nouvelles versions de logiciels Apple sont disponibles.
NO_BONJOUR=1	Ne pas installer Bonjour. Bonjour fournit la découverte sans configuration de réseaux d'imprimantes, de bibliothèques iTunes partagées et d'autres services.
NO_QUICKTIME=1	Ne pas installer QuickTime. Ce composant est obligatoire pour utiliser iTunes. N'omettez pas QuickTime à moins d'être sûr que la dernière version est déjà installée sur l'ordinateur client.

Installation silencieuse sous Windows

Pour installer iTunes sans intervention, extrayez les différents fichiers .msi d'iTunesSetup.exe, puis transmettez les fichiers par push data aux ordinateurs clients.

Pour extraire des fichiers .msi d'iTunesSetup.exe :

1. Exécutez iTunesSetup.exe.
2. Ouvrez *%temp%* et recherchez le dossier intitulé IXP*nnn*.TMP, où *%temp%* correspond à votre répertoire temporaire et *nnn* à un nombre aléatoire à trois chiffres. Sous Windows XP, le répertoire temporaire correspond généralement à *lecteur_démarrage*:\Documents and Settings*utilisateur*\Local Settings\temp\. Sous Windows Vista, ce répertoire est d'habitude \Users*utilisateur*\AppData\Local\Temp\.
3. Copiez les fichiers .msi du dossier dans un autre emplacement.
4. Quittez le programme d'installation ouvert par iTunesSetup.exe.

Utilisez ensuite Group Policy Object Editor, dans Microsoft Management Console, pour ajouter les fichiers .msi à une politique de configuration d'ordinateur. Ajoutez bien la configuration au règlement de configuration d'ordinateur et non au règlement de configuration d'utilisateur.

Important : iTunes requiert QuickTime et Application Support d'Apple. Application Support d'Apple doit être installé avant d'installer iTunes. « Apple Mobile Device Services » (AMDS) est nécessaire pour utiliser un iPod touch, un iPad ou un iPhone avec iTunes.

Avant de transmettre par push data les fichiers .msi, vous devez sélectionner les versions localisées d'iTunes à installer. Pour ce faire, ouvrez le .msi dans l'outil Orca installé par le SDK de Windows sous le nom Orca.msi, dans le dossier bin\. Modifiez ensuite le flux des informations du résumé et supprimez les langues que vous n'avez pas besoin d'installer. (Locale ID1033 correspond à l'anglais.) Une autre solution consiste à faire appel à l'Éditeur d'objets de stratégie de groupe pour faire passer les propriétés de déploiement des fichiers .msi sur Ignorer la langue.

Installation d'iTunes sur des ordinateurs Macintosh

Les ordinateurs Mac sont fournis avec iTunes installé. La dernière version d'iTunes est disponible à l'adresse www.itunes.fr. Pour transmettre iTunes sur des clients Mac par push data, vous pouvez utiliser Gestionnaire de groupe de travail, un outil administratif fourni avec Mac OS X Server.

Activation rapide des appareils avec iTunes

Avant de pouvoir utiliser un nouvel iPhone, iPod touch ou iPad, il est nécessaire de l'activer en le branchant sur un ordinateur exécutant iTunes. Après l'activation d'un appareil, iTunes propose normalement de le synchroniser avec l'ordinateur. Pour éviter ceci lorsque vous configurez un appareil pour une autre personne, activez le mode d'activation seule. iTunes éjecte alors automatiquement les appareils après leur activation. L'appareil est alors prêt à être configuré mais il ne possède aucune donnée.

Pour activer le mode d'activation seule sur Mac OS X :

1. Assurez-vous qu'iTunes n'est pas en cours d'exécution, puis ouvrez Terminal.
2. Dans Terminal, saisissez une commande :
   - Pour activer le mode d'activation seule :

     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 1
     ```
   - Pour désactiver le mode d'activation seule :

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

Pour activer un appareil, consultez « Utilisation du mode d'activation seule » ci-dessous.

Pour activer le mode d'activation seule sur Windows :

1. Assurez-vous qu'iTunes n'est pas en cours d'exécution, puis ouvrez une fenêtre d'invite de commande.
2. Saisissez une commande :
   - Pour activer le mode d'activation seule :

     ```
     C:\Program Files\iTunes\iTunes.exe /setPrefInt StoreActivationMode 1
     ```
   - Pour désactiver le mode d'activation seule :

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

Vous pouvez également créer un raccourci ou modifier le raccourci iTunes que vous possédez déjà pour inclure ces commandes afin de pouvoir activer ou désactiver rapidement le mode d'activation seule.

Pour vous assurer qu'iTunes est bien en mode d'activation seule, choisissez iTunes > À propos d'iTunes, et lancez une recherche par le texte « mode activation seule », sous la version et l'identifiant d'iTunes.

Utilisation du mode d'activation seule

Assurez-vous d'avoir activé le mode d'activation seule comme décrit ci-dessus, puis suivez les étapes suivantes.

1. Si vous activez un iPhone, insérez une carte SIM activée. Utilisez l'outil d'éjection SIM ou un trombone déplié pour éjecter le support pour carte SIM. Consultez le *Guide de l'utilisateur d'iPhone* pour en savoir plus.
2. Branchez l'iPhone, l'iPod touch ou l'iPad sur l'ordinateur. L'ordinateur doit être connecté à Internet afin d'activer l'appareil.

   iTunes s'ouvre, si nécessaire, et active l'appareil. Un message apparaît lorsque l'appareil a été activé.
3. Débranchez l'appareil.

   Vous pouvez brancher et activer immédiatement d'autres appareils. iTunes n'effectue de synchronisation avec aucun appareil tant que le mode d'activation seule est en vigueur. N'oubliez donc pas de désactiver ce mode si vous comptez utiliser iTunes pour synchroniser des appareils.

Définition de restrictions iTunes

Vous pouvez empêcher vos utilisateurs d'utiliser certaines fonctionnalités d'iTunes. On appelle parfois cela les contrôles parentaux. Les fonctionnalités suivantes peuvent être contrôlées :

- recherche automatique et manuelle de nouvelles versions d'iTunes et de mises à jour de logiciels pour appareil.
- Affichage des propositions Genius pendant le parcours ou la lecture de données multimédias
- Synchronisation automatique lorsque des appareils sont connectés
- Téléchargement de l'illustration des albums
- Utilisation de modules du visualiseur
- Saisie d'une URL de diffusion en continu de données
- Découverte automatique de systèmes Apple TV
- Enregistrement de nouveaux appareils auprès d'Apple
- Inscription à des podcasts
- Lecture de la radio par Internet

- Accès à l'iTunes Store
- Partage de bibliothèque avec des ordinateurs du réseau local et exécutant aussi iTunes
- Lecture de contenus iTunes marqués comme explicites
- Lecture de films
- Lecture d'émissions télé

Définition de restrictions iTunes pour Mac OS X

Sous Mac OS X, l'on contrôle l'accès à l'aide de clés dans un fichier plist. Sous Mac OS X, les valeurs de clé illustrées ci-avant peuvent être spécifiées pour chaque utilisateur en modifiant ~/Bibliothèque/Preferences/com.apple.iTunes.plist à l'aide de Gestionnaire de groupe de travail, un outil administratif fourni avec Mac OS X Server.

Pour obtenir des instructions, consultez l'article du support d'Apple à l'adresse http://docs.info.apple.com/article.html?artnum=303099 (en anglais).

Définition de restrictions iTunes pour Windows

Sous Windows, l'on contrôle l'accès en définissant des valeurs de registre dans une des clés de registre suivantes :

Sous Windows XP et Windows Vista 32 bits :

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

Sous Windows Vista 64 bits :

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

Pour en savoir plus sur les valeurs de registre iTunes, consultez l'article Apple Support à l'adresse http://support.apple.com/kb/HT2102?locale=fr_FR (en anglais).

Pour consulter des informations d'ordre général sur la modification du registre Windows, consultez l'article Microsoft Aide et Support à l'adresse http://support.microsoft.com/kb/136393.

Mise à jour manuelle d'iTunes et du système d'exploitation de l'iPhone

Si vous désactivez la recherche de mises à jour de logiciels automatique et manuelle iTunes, vous devez distribuer les mises à jour de logiciels aux utilisateurs pour une installation manuelle.

Pour mettre à jour iTunes, consultez les instructions d'installation et de déploiement plus haut dans ce document. Le processus est le même que celui qui permet de distribuer iTunes à vos utilisateurs.

Pour mettre à jour le système d'exploitation de l'iPhone, procédez comme suit :

1. Sur un ordinateur sur lequel la mise à jour de logiciels iTunes n'est pas désactivée, utilisez iTunes pour télécharger la mise à jour de logiciels . Pour ce faire, sélectionnez un appareil attaché dans iTunes, cliquez sur l'onglet Résumé, puis cliquez sur le bouton « Rechercher les mises à jour ».
2. Après le téléchargement, copiez le fichier du programme de mise à jour (.ipsw) qui se trouve dans l'emplacement suivant :
   - *Sous Mac OS X :* ~/Bibliothèque/iTunes/iPhone Software Updates/
   - *Sous Windows XP :* *lecteur_de_démarrage*:\Documents and Settings*utilisateur*\Application Data\Apple Computer\iTunes\iPhone Software Updates\
3. Distribuez le fichier .ipsw à vos utilisateurs ou placez-le sur un lecteur réseau où ils peuvent y accéder.
4. Demandez à vos utilisateurs de sauvegarder leur appareil à l'aide d'iTunes avant d'appliquer la mise à jour. Pendant les mises à jour manuelles, iTunes ne sauvegarde pas automatiquement l'appareil avant l'installation. Pour créer une nouvelle sauvegarde, cliquez avec le bouton droit de la souris (Windows) ou cliquez tout en maintenant la touche Contrôle enfoncée (Mac) sur l'appareil dans la barre latérale d'iTunes. Choisissez ensuite Sauvegarder dans le menu contextuel qui apparaît.
5. Vos utilisateurs installent la mise à jour en connectant leur appareil à iTunes, puis en sélectionnant l'onglet Résumé pour leur appareil. Ils maintiennent ensuite enfoncée la touche Option (Mac) ou Maj (Windows) et cliquent sur le bouton « Rechercher les mises à jour ».
6. Une zone de dialogue de sélection de fichier apparaît. Les utilisateurs doivent sélectionner le fichier .ipsw puis cliquer sur Ouvrir pour lancer le processus de mise à jour.

Sauvegarde de votre appareil sur iTunes

Lorsque votre iPhone, iPod touch ou iPad se synchronise avec iTunes, les réglages de l'appareil sont automatiquement sauvegardés sur l'ordinateur. Les applications achetées auprès de l'App Store sont copiées dans la bibliothèque iTunes.

Les applications que vous développez vous-mêmes et distribuez aux utilisateurs par le biais des profils de distribution d'entreprise ne sont ni sauvegardées, ni transférées sur l'ordinateur de l'utilisateur. En revanche, la sauvegarde de l'appareil comprend tous les fichiers créés par ces applications.

Vous pouvez stocker les copies de sauvegarde d'appareil sous un format chiffré en sélectionnant, dans iTunes puis la sous-fenêtre de résumé des appareils, l'option « Chiffrer la sauvegarde ». Les fichiers sont encryptés en AES256. Cette clé est stockée de façon sécurisée dans le trousseau de l'iPhone OS.

Important : si l'appareil en cours de sauvegarde comprend des profils chiffrés installés, iTunes impose à l'utilisateur d'activer le chiffrement des copies de sauvegarde.

Déploiement d'applications

5

Vous pouvez distribuer des applications iPhone, iPod touch et iPad à vos utilisateurs.

Si vous voulez installer des applications iPhone OS que vous avez développées, distribuez les applications à vos utilisateurs, qui installent les applications à l'aide d'iTunes.

Les applications de l'App Store en ligne fonctionnent directement sur l'iPhone, l'iPod touch et l'iPad. Si vous développez une application que vous voulez distribuer vous-même, elle doit être signée numériquement à l'aide d'un certificat émis par Apple. Vous devez également fournir à vos utilisateurs un profil d'approvisionnement de distribution qui permet à leur appareil d'utiliser l'application.

Le processus de déploiement de vos propres applications est le suivant :

- Inscrivez-vous pour le développement d'entreprise auprès d'Apple.
- Signez vos applications à l'aide de votre certificat.
- Créez un profil d'approvisionnement de distribution d'entreprise qui autorise les appareils à utiliser les applications que vous avez signées.
- Déployez l'application et le profil d'approvisionnement de distribution d'entreprise sur les ordinateurs de vos utilisateurs.
- Signalez à vos utilisateurs qu'ils doivent installer l'application et le profil à l'aide d'iTunes.

Pour en savoir plus sur les différentes étapes, lisez ce qui suit.

Inscription au développement d'applications

Pour développer et déployer des applications personnalisées pour l'iPhone OS, vous devez vous inscrire au programme Enterprise Developer à l'adresse http://developer.apple.com/ (en anglais).

Au terme du processus d'inscription, vous recevrez des instructions sur la manière de faire fonctionner vos applications sur des appareils.

Signature d'applications

Les applications que vous distribuez à des utilisateurs doivent être signées à l'aide de votre certificat de distribution. Pour obtenir des instructions sur l'obtention et l'utilisation d'un certificat, consultez l'iPhone Developer Center à l'adresse http://developer.apple.com/iphone (en anglais).

Création d'un profil d'approvisionnement de distribution

Les profils d'approvisionnement de distribution vous permettent de créer des applications que vos utilisateurs peuvent utiliser sur leur appareil. L'on crée un profil d'approvisionnement de distribution d'entreprise pour une application spécifique ou pour plusieurs applications en spécifiant l'AppID qui est autorisé par le profil. Si un utilisateur dispose d'une application, mais pas du profil qui en autorise l'utilisation, l'utilisateur ne peut pas utiliser l'application.

L'agent d'équipe désigné pour votre entreprise peut créer des profils d'approvisionnement de distribution dans le portail Enterprise Program Portal à l'adresse http://developer.apple.com/iphone (en anglais). Consultez le site web pour obtenir des instructions.

Une fois que vous avez créé le profil d'approvisionnement de distribution d'entreprise, téléchargez le fichier .mobileprovision puis distribuez le fichier et votre application de manière sécurisée.

Installation de profils d'approvisionnement à l'aide d'iTunes

L'exemplaire d'iTunes de l'utilisateur installe automatiquement des profils d'approvisionnement dans les dossiers mentionnés dans cette rubrique. Si les dossiers n'existent pas, créez-les avec le nom indiqué.

Mac OS X

- ~/Bibliothèque/MobileDevice/Provisioning Profiles/
- /Bibliothèque/MobileDevice/Provisioning Profiles/
- le chemin spécifié par la clé ProvisioningProfilesPath dans ~/Bibliothèque/Preferences/com.apple.itunes

Windows XP

- *lecteur_de_démarrage*:\Documents and Settings*nom_d'utilisateur*\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- *lecteur_de_démarrage*:\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- le chemin spécifié dans le HKCU ou HKLM par la clé de registre ProvisioningProfilesPath SOFTWARE\Apple Computer, Inc\iTunes

Windows Vista

- *lecteur_de_démarrage*:\Users*nom _d'utilisateur*\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *lecteur_de_démarrage*:\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- le chemin spécifié dans le HKCU ou HKLM par la clé de registre ProvisioningProfiles-Path SOFTWARE\Apple Computer, Inc\iTunes

iTunes installe automatiquement les profils d'approvisionnement qui se trouvent dans les emplacements ci-dessus sur les appareils avec lesquels il se synchronise. Une fois installés, les profils d'approvisionnement peuvent être affichés sur l'appareil dans Réglages > Général > Profils.

Vous pouvez également distribuer le fichier .mobileprovision à vos utilisateurs et leur demander de le faire glisser sur l'icône de l'application iTunes. iTunes copie alors le fichier dans le bon emplacement décrit ci-dessus.

Installation de profils d'approvisionnement à l'aide d'« Utilitaire de configuration iPhone »

Vous pouvez utiliser « Utilitaire de configuration iPhone » pour installer des profils d'approvisionnement sur les appareils connectés. Procédez comme suit :

1. Dans « Utilitaire de configuration iPhone », choisissez Fichier > Ajouter à la bibliothèque, puis sélectionnez le profil d'approvisionnement à installer.

   Le profil est ajouté à « Utilitaire de configuration iPhone » et peut être affiché en sélectionnant la catégorie Profils d'approvisionnement dans la bibliothèque.
2. Sélectionnez un appareil dans la liste Appareils connectés.
3. Cliquez sur l'onglet Profils d'approvisionnement.
4. Sélectionnez le profil d'approvisionnement dans la liste puis cliquez sur son bouton Installer.

Installation d'applications à l'aide d'iTunes

Vos utilisateurs peuvent utiliser iTunes pour installer des applications sur leurs appareils. Distribuez l'application à vos utilisateurs de manière sécurisée et demandez-leur de procéder comme suit :

1. Dans iTunes, choisissez Fichier > Ajouter à la bibliothèque puis sélectionnez l'application (.app) que vous avez fournie.

   Vous pouvez également faire glisser le fichier .app vers l'icône de l'application iTunes.
2. Connectez un appareil à l'ordinateur puis sélectionnez-le dans la liste Appareils dans iTunes.

3 Cliquez sur l'onglet Applications, puis sélectionnez l'application dans la liste.

4 Cliquez sur Appliquer pour installer l'application et tous les profils d'approvisionnement de distribution qui se trouvent dans les dossiers désignés décrits dans « Installation de profils d'approvisionnement à l'aide d'iTunes » à la page 70.

Installation d'applications à l'aide d'« Utilitaire de configuration iPhone »

Vous pouvez utiliser « Utilitaire de configuration iPhone » pour installer des applications sur les appareils connectés. Procédez comme suit :

1 Dans « Utilitaire de configuration iPhone », choisissez Fichier > Ajouter à la bibliothèque, puis sélectionnez l'application à installer.

L'application est ajoutée à « Utilitaire de configuration iPhone » et peut être affichée en sélectionnant la catégorie Applications dans la bibliothèque.

2 Sélectionnez un appareil dans la liste Appareils connectés.

3 Cliquez sur l'onglet Applications.

4 Sélectionnez l'application dans la liste, puis cliquez sur son bouton Installer.

Utilisation d'applications d'entreprise

Lorsqu'un utilisateur exécute une application qui n'est pas signée par Apple, l'appareil recherche un profil d'approvisionnement de distribution qui en autorise l'utilisation. S'il n'en trouve pas, l'application ne s'ouvre pas.

Désactivation d'une application d'entreprise

Si vous cherchez à désactiver une application interne, vous pouvez procéder en révoquant l'identité servant à signer le profil d'approvisionnement de distribution. Plus personne n'est alors en mesure d'installer l'application et, si cette dernière était déjà installée, elle ne peut plus s'ouvrir.

Autres ressources

Pour en savoir plus sur la création d'applications et de profils d'approvisionnement, consultez :

- l'iPhone Developer Center à l'adresse http://developer.apple.com/iphone (en anglais)

Configuration d'un serveur VPN Cisco

Utilisez ces instructions qui suivent pour configurer votre serveur VPN Cisco pour pouvoir l'utiliser avec l'iPhone, l'iPod touch et l'iPad.

Plate-formes Cisco prises en charge

Le système d'exploitation iPhone OS prend en charge les appareils de sécurité Cisco ASA 5500 et les coupe-feu PIX configurés avec le logiciel 7.2.x ou ultérieur. La dernière version du logiciel 8.0.x (ou ultérieur) est recommandée. iPhone OS prend aussi en charge les routeurs VPN Cisco IOS avec IOS 12.4(15)T ou ultérieur. Les concentrateurs VPN 3000 Series ne prennent pas en charge les fonctionnalités VPN de l'iPhone.

Méthodes d'authentification

Le système d'exploitation iPhone OS prend en charge les méthodes d'authentification suivantes :

- L'authentification IPsec par clé prépartagée avec authentification des utilisateurs par xauth.
- Les certificats client et serveur pour l'authentification IPsec avec authentification des utilisateurs facultative par xauth.
- L'authentification hybride où le serveur fournit un certificat et le client fournit une clé prépartagée pour l'authentification IPsec ; l'authentification de l'utilisateur est requise via xauth.
- L'authentification des utilisateurs est fournie par xauth et couvre les méthodes d'authentification suivantes :
  - Nom d'utilisateur avec mot de passe
  - RSA SecurID
  - CryptoCard

Groupes d'authentification

Le protocole Cisco Unity utilise des groupes d'authentification pour regrouper les utilisateurs en fonction d'un jeu commun de paramètres d'authentification et d'autres paramètres. Il est recommandé de créer un groupe d'authentification pour les utilisateurs d'appareils basés sur le système d'exploitation iPhone OS. Pour l'authentification hybride et par clé prépartagée, le nom du groupe doit être configuré sur l'appareil avec le secret partagé (clé prépartagée) comme mot de passe du groupe.

Lorsque l'on utilise l'authentification par certificat, aucun secret partagé n'est utilisé et le groupe de l'utilisateur est déterminé en fonction de certains champs du certificat. Les réglages du serveur Cisco peuvent être utilisés pour mettre en correspondance des champs du certificat avec des groupes d'utilisateurs.

Certificats

Lors de la configuration et de l'installation de certificats, assurez-vous des points suivants :

- Le certificat d'identité du serveur doit contenir le nom DNS et/ou l'adresse IP du serveur dans le champ pour le nom alternatif de sujet (SubjectAltName). L'appareil utilise cette information pour vérifier que le certificat appartient bien au serveur. Vous pouvez spécifier le nom alternatif de sujet en utilisant des caractères de remplacement pour la mise en correspondance segment par segment, par exemple, vpn.*.mon_entreprise.com, pour plus de flexibilité. Vous pouvez mettre le nom DNS dans le champ pour le nom commun si vous ne spécifiez pas le nom alternatif de sujet.
- Le certificat de l'autorité de certificat qui a signé le certificat du serveur devrait être installé sur l'appareil. S'il ne s'agit pas d'un certificat racine, installez le reste de la chaîne de confiance afin que la confiance soit accordée au certificat.
- Si des certificats clients sont utilisés, vérifiez que le certificat de l'autorité de certificat de confiance qui a signé le certificat du client est bien installé sur le serveur VPN.
- Les certificats et les autorités de certificat doivent être valides (pas arrivés à expiration, par exemple).
- L'envoi de chaînes de certificat par le serveur n'est pas pris en charge et devrait être désactivé.
- Lors de l'utilisation d'une authentification par certificats, vérifiez que le serveur est bien configuré pour identifier le groupe d'utilisateurs sur la base des champs du certificat client. Consultez « Groupes d'authentification » à la page 74.

Réglages IPSec

Utilisez les réglages IPSec suivants :

- *Mode :* mode tunnel
- *Modes d'échange de clés par Internet :* mode agressif pour l'authentification par clé prépartagée et hybride, mode principal pour l'authentification par certificat.
- *Algorithmes de chiffrement :* 3DES, AES-128, AES-256
- *Algorithmes d'authentification :* HMAC-MD5, HMAC-SHA1
- *Groupes Diffie Hellman :* le groupe 2 est obligatoire pour l'authentification par clé pré-partagée et l'authentification hybride. Pour l'authentification par certificat, utilisez le groupe 2 avec 3DES et AES-128. Utilisez le groupe 2 ou 5 avec AES-256.
- *PFS (Perfect Forward Secrecy) :* pour l'échange de clés par Internet (IKE) hase 2, si PFS est utilisé, le groupe Diffie-Hellman doit être le même que celui qui était utilisé pour IKE phase 1.
- *Configuration du mode :* doit être activée.
- *Détection des pairs morts :* recommandée.
- *Transversal NAT standard :* pris en charge et peut être activé si nécessaire. (IPSec sur TCP n'est pas pris en charge).
- *Équilibrage de la charge :* pris en charge et peut être activé si nécessaire.
- *Recomposition de la phase 1 :* pas pris en charge pour le moment. Il est recommandé de régler les temps de recomposition sur le serveur sur approximativement une heure.
- *Masque d'adresse ASA :* assurez-vous que le masque de réserve d'adresse de tous les appareils n'est pas défini ou qu'il l'est sur 255.255.255.255. Par exemple :

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

  Lorsque le masque d'adresse recommandé est utilisé, certaines routes utilisées par la configuration VPN sont susceptibles d'être ignorées. Pour éviter cela, assurez-vous que votre tableau de routage contient toutes les routes nécessaires et vérifiez que les adresses de sous-réseau sont accessibles avant le déploiement.

Autres fonctionnalités prises en charge

L'iPhone, l'iPod touch et l'iPad prennent en outre en charge les fonctionnalités suivantes :

- *Version d'application :* la version du logiciel client est envoyée au serveur, ce qui lui permet d'accepter ou de rejeter des connexions en fonction de la version du logiciel de l'appareil.
- *Bannière :* la bannière, si elle est configurée sur le serveur, est affichée sur l'appareil et l'utilisateur doit l'accepter ou se déconnecter.
- *Split Tunnel :* le « split tunneling » est pris en charge.
- *Split DNS :* le « split DNS » est pris en charge.
- *Domaine par défaut :* le domaine par défaut est pris en charge.

Format des profils de configuration

La présente annexe décrit le format des fichiers mobileconfig pour ceux qui veulent créer leurs propres outils.

Le présent document assume que vous connaissez le DTD XML d'Apple et le format de liste de propriétés général. Une description générale du format plist d'Apple est disponible à l'adresse www.apple.com/DTDs/PropertyList-1.0.dtd. Pour commencer, utilisez « Utilitaire de configuration iPhone » pour créer un fichier squelette que vous pouvez modifier à l'aide des informations incluses dans cette annexe.

Le présent document utilise les termes *donnée utile* et *profil*. Un profil est un fichier entier qui configure certains réglages (individuels ou multiples) sur un iPhone, un iPod touch ou un iPad. Une donnée utile est un composant individuel du fichier de profil.

Niveau de la racine

Au niveau de la racine, le fichier de configuration est un dictionnaire contenant les paires clé-valeur suivantes :

Clé	Valeur
PayloadVersion	Nombre, obligatoire. Version du fichier du profil de configuration dans son ensemble. Ce numéro de version désigne le format du profil dans son ensemble, pas des différentes données utiles.
PayloadUUID	Chaîne, obligatoire. Il s'agit généralement d'une chaîne d'identification unique générée artificiellement. Le contenu exact de cette chaîne est sans importance mais elle doit être globalement unique. Sur Mac OS X, vous pouvez créer des UUID avec /usr/bin/uuidgen.
PayloadType	Chaîne, obligatoire. Pour le moment, la seule valeur valide pour cette clé est « Configuration ».
PayloadOrganization	Chaîne, facultatif. Cette valeur décrit l'organisation en matière d'émission du profil, telle qu'elle est visible par l'utilisateur.

Clé	Valeur
PayloadIdentifier	Chaîne, obligatoire. Cette valeur est, par convention, une chaîne délimitée par des points décrivant de manière univoque le profil, comme « com.mon_entreprise.iPhone.reglages_courrier » ou « edu.mon_universite.etudiants.vpn ». Il s'agit de la chaîne permettant de distinguer les différents profils entre eux. Si un profil dont l'identifiant correspond à un autre profil est installé, le premier écrase le second (au lieu d'être ajouté).
PayloadDisplayName	Chaîne, obligatoire. Cette valeur détermine la chaîne très courte décrivant le profil à présenter à l'utilisateur, comme « Réglages VPN ». Elle ne doit pas être unique.
PayloadDescription	Chaîne, facultatif. Cette valeur détermine le texte descriptif libre qui doit être présenté à l'utilisateur à l'écran Détail pour le profil dans son ensemble. Cette chaîne devrait identifier clairement le profil afin que l'utilisateur puisse déterminer s'il doit l'installer ou pas.
PayloadContent	Matrice, facultatif. Cette valeur est le contenu proprement dit du profil. Si elle est omise, le profil dans son ensemble n'a pas de signification fonctionnelle.
PayloadRemovalDisallowed	Booléen, facultatif. La valeur par défaut est « No ». Une fois définie, l'utilisateur ne peut pas supprimer le profil. Un profil ainsi défini ne peut être mis à jour à travers une connexion USB ou par le biais du web/courrier électronique que si l'identifiant du profil concorde et est signé par la même autorité. Si un mot de passe de suppression est fourni, celui-ci permet de supprimer le profil. Grâce à la signature et au chiffrement des profils, ce bit de verrouillage en clair reste sans conséquence car le profil n'est pas modifiable et car ce réglage est également affiché sur l'appareil.

Contenu des données utiles

La matrice PayloadContent est une matrice de dictionnaires dans laquelle chaque dictionnaire décrit une donnée utile individuelle du profil. Chaque profil fonctionnel possède au moins une entrée dans la matrice. Tous les dictionnaires de cette matrice ont quelques propriétés en commun quel que soit le type de donnée utile. D'autres sont spécialisés et uniques à un type de donnée utile.

Clé	Valeur
PayloadVersion	Nombre, obligatoire. Version de la donnée utile individuelle. Un profil peut contenir des données utiles de différentes versions. Par exemple, le numéro de la version du VPN pourra être incrémenté à l'avenir alors que la version de Mail ne le sera pas.
PayloadUUID	Chaîne, obligatoire. Il s'agit généralement d'une chaîne d'identification unique générée artificiellement. Le contenu exact de cette chaîne est sans importance mais elle doit être globalement unique.

Clé	Valeur
PayloadType	Chaîne, obligatoire. Cette paire clé-valeur détermine le type de donnée utile individuelle au sein du profil.
PayloadOrganization	Chaîne, facultatif. Cette valeur décrit l'organisation en matière d'émission du profil, telle qu'elle sera présentée à l'utilisateur. Elle peut mais ne doit pas être identique à celle de PayloadOrganization au niveau de la racine.
PayloadIdentifier	Chaîne, obligatoire. Cette valeur est, par convention, une chaîne délimitée par des points décrivant de manière univoque la donnée utile. Il s'agit généralement du paramètre PayloadIdentifier de la racine dont le sous-identifiant est ajouté en suffixe. Cette association de données décrit la donnée utile en question.
PayloadDisplayName	Chaîne, obligatoire. Cette valeur est une chaîne très courte présentée à l'utilisateur qui décrit le profil, comme « Réglages VPN ». Elle ne doit pas être unique.
PayloadDescription	Chaîne, facultatif. Cette valeur détermine le texte descriptif libre à afficher à l'écran Détail pour la donnée utile en question.

Donnée utile Profile Removal Password

La donnée utile Removal Password est désignée par la valeur de PayloadType « com.apple.profileRemovalPassword ». Son but est d'encoder le mot de passe permettant aux utilisateurs de supprimer un profil de configuration à partir de l'appareil. Si cette donnée utile est présente et si la valeur du mot de passe est définie, l'appareil exige alors le mot de passe lorsque l'utilisateur active un bouton de suppression du profil. Cette donnée utile est chiffrée avec le reste du profil.

Clé	Valeur
RemovalPassword	Chaîne, facultatif. Spécifie le mot de passe de suppression du profil.

Donnée utile Passcode Policy

La donnée utile Passcode Policy est désignée par la valeur PayloadType com.apple.mobiledevice.passwordpolicy. La présence de ce type de donnée utile invite l'appareil à présenter à l'utilisateur un mécanisme de saisie de code alphanumérique qui permet de saisir des codes complexes de longueur arbitraire.

En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
allowSimple	Booléen, facultatif. La valeur par défaut est « YES ». Détermine si un code simple est autorisé. Un code simple est défini comme une chaîne contenant des caractères qui se répètent ou des caractères consécutifs ascendants ou descendants (comme 123 ou CBA). Régler cette valeur sur « NO » équivaut à régler minComplexChars sur « 1 ».
forcePIN	Booléen, facultatif. La valeur par défaut est « NO ». Détermine si l'utilisateur doit définir un numéro d'identification personnel (PIN). Régler simplement cette valeur (et aucune autre) force l'utilisateur à saisir un code sans imposer de longueur ni de qualité.
maxFailedAttempts	Nombre, facultatif. La valeur par défaut est 11. Plage autorisée [2…11]. Spécifie le nombre de tentatives autorisées pour la saisie du code à l'écran verrouillé de l'appareil. Une fois que ce nombre est dépassé, l'appareil est verrouillé et doit être connecté à son iTunes désigné pour être déverrouillé.
maxInactivity	Nombre, facultatif. La valeur par défaut est « Infinity ». Spécifie le nombre de minutes pendant lesquelles l'appareil peut rester inactif (sans que l'utilisateur le déverrouille) avant d'être verrouillé par le système. Une fois que cette limite est atteinte, l'appareil est verrouillé et le code doit être saisi.
maxPINAgeInDays	Nombre, facultatif. La valeur par défaut est « Infinity ». Spécifie le nombre de jours pendant lequel le code ne doit pas être modifié. Après ce nombre de jours, l'utilisateur est obligé de changer le code avant que l'appareil ne soit déverrouillé.
minComplexChars	Nombre, facultatif. La valeur par défaut est 0. Spécifie le nombre minimum de caractères complexes que le code doit contenir. Un caractère « complexe » est un caractère autre qu'un chiffre ou une lettre, comme &%$#.
minLength	Nombre, facultatif. La valeur par défaut est 0. Spécifie la longueur totale minimum du code. Ce paramètre est indépendant de l'argument facultatif lui aussi minComplexChars.
requireAlphanumeric	Booléen, facultatif. La valeur par défaut est « NO ». Spécifie si l'utilisateur doit saisir des caractères alphabétiques (« abcd ») ou si des chiffres suffisent.
pinHistory	Nombre, facultatif. Si l'utilisateur modifie le mot de passe, il doit faire en sorte que ce dernier est unique dans les N dernières entrées de l'historique. La valeur minimale est 1, la valeur maximale est 50.

Clé	Valeur
manualFetchingWhenRoaming	Booléen, facultatif. Une fois définie, toutes les opérations push sont désactivées en mode d'itinérance. L'utilisateur doit récupérer manuellement de nouvelles données.
maxGracePeriod	Nombre, facultatif. Le délai maximal, en minutes, permettant de déverrouiller le téléphone sans avoir à saisir de code. La valeur par défaut est 0. Si aucun délai n'est précisé, un code est immédiatement demandé.

Donnée utile Email

La donnée utile Email est désignée par la valeur PayloadType com.apple.mail.managed. Cette donnée utile crée un compte de messagerie sur l'appareil. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
EmailAccountDescription	Chaîne, facultatif. Une description visible par l'utilisateur du compte de messagerie affichée dans les applications Mail et Réglages.
EmailAccountName	Chaîne, facultatif. Nom d'utilisateur complet du compte. Il s'agit du nom d'utilisateur qui apparaît dans les messages envoyés, etc.
EmailAccountType	Chaîne, obligatoire. Les valeurs autorisées sont EmailTypePOP et EmailTypeIMAP. Définit le protocole à utiliser pour ce compte.
EmailAddress	Chaîne, obligatoire. Désigne l'adresse électronique complète du compte. Si cette clé n'apparaît pas dans la donnée utile, l'appareil invite à saisir cette chaîne pendant l'installation du profil.
IncomingMailServerAuthentication	Chaîne, obligatoire. Désigne le schéma d'authentification pour le courrier entrant. Les valeurs autorisées sont EmailAuthPassword et EmailAuthNone.
IncomingMailServerHostName	Chaîne, obligatoire. Désigne le nom d'hôte (ou l'adresse IP) du serveur de courrier entrant.
IncomingMailServerPortNumber	Nombre, facultatif. Désigne le numéro de port du serveur de courrier entrant. Si aucun numéro de port n'est spécifié, c'est le port par défaut du protocole qui est utilisé.
IncomingMailServerUseSSL	Booléen, facultatif. La valeur par défaut est « YES ». Spécifie si le serveur de courrier entrant utilise SSL pour l'authentification.
IncomingMailServerUsername	Chaîne, obligatoire. Désigne le nom d'utilisateur du compte de messagerie, généralement l'adresse électronique jusqu'au caractère @. Si elle n'apparaît pas dans la donnée utile et si le compte est configuré de manière à exiger l'authentification pour le courrier entrant, l'appareil invite à saisir cette chaîne pendant l'installation du profil.
IncomingPassword	Chaîne, facultatif. Mot de passe pour le serveur de courrier entrant. À utiliser uniquement avec des profils chiffrés.

Clé	Valeur
OutgoingPassword	Chaîne, facultatif. Mot de passe pour le serveur de courrier sortant. À utiliser uniquement avec des profils chiffrés.
OutgoingPasswwordSameAsIncomingPassword	Booléen, facultatif. Lorsque le mot de passe est défini, l'utilisateur est invité à le saisir une seule fois, que ce soit pour les messages sortants ou entrants.
OutgoingMailServerAuthentication	Chaîne, obligatoire. Désigne le schéma d'authentification pour le courrier sortant. Les valeurs autorisées sont EmailAuthPassword et EmailAuthNone.
OutgoingMailServerHostName	Chaîne, obligatoire. Désigne le nom d'hôte (ou l'adresse IP) du serveur de courrier sortant.
OutgoingMailServerPortNumber	Nombre, facultatif. Désigne le numéro de port du serveur de courrier sortant. Si aucun numéro de port n'est spécifié, ce sont les ports 25, 587 et 465 qui sont utilisés, dans cet ordre.
OutgoingMailServerUseSSL	Booléen, facultatif. La valeur par défaut est « YES ». Spécifie si le serveur de courrier sortant utilise SSL pour l'authentification.
OutgoingMailServerUsername	Chaîne, obligatoire. Désigne le nom d'utilisateur du compte de messagerie, généralement l'adresse électronique jusqu'au caractère @. Si elle n'apparaît pas dans la donnée utile et si le compte est configuré de manière à exiger l'authentification pour le courrier sortant, l'appareil invite à saisir cette chaîne pendant l'installation du profil.

Donnée utile Web Clip

La donnée utile Web Clip est désignée par la valeur PayloadType com.apple.webClip.managed. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
URL	Chaîne, obligatoire. URL s'ouvrant après avoir cliqué sur le clip web. L'URL doit commencer par HTTP ou HTTPS pour être valide.
Label	Chaîne, obligatoire. Nom du clip web tel qu'il s'affiche sur l'écran d'accueil.
Icon	Données, facultatif. Icône PNG à afficher sur l'écran d'accueil. Sa taille doit être de 59 x 60 pixels. Si aucune icône n'est indiquée, un carré blanc s'affiche alors.
IsRemovable	Booléen, facultatif. Dans le cas contraire, l'utilisateur ne peut pas procéder à la suppression du clip, qui ne peut se faire qu'à la suppression du profil.

Donnée utile Restrictions

La donnée utile Restrictions est désignée par la valeur PayloadType com.apple.applicationaccess . En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
allowAppInstallation	Booléen, facultatif. Si cette option est définie sur false, l'accès au magasin en ligne App Store est désactivé et son icône est retirée du menu principal. L'utilisateur est en outre dans l'impossibilité d'installer ou de mettre à jour ses applications.
allowCamera	Booléen, facultatif. Si cette option est définie sur false, l'appareil photo est totalement désactivé et son icône est supprimée de l'écran d'accueil. L'utilisateur est alors dans l'impossibilité de prendre des photos.
allowExplicitContent	Booléen, facultatif. Si cette option est définie sur false, les morceaux de musique et les vidéos au contenu explicite achetés sur l'iTunes Store sont masqués. Les éléments réservés à un public averti sont clairement indiqués, d'après les données procurées par leur fournisseur, par exemple un label musical, au moment de leur vente à travers l'iTunes Store.
allowScreenShot	Booléen, facultatif. Si cette option est définie sur false, l'utilisateur est dans l'impossibilité d'enregistrer une capture de l'écran.
allowYouTube	Booléen, facultatif. Si cette option est définie sur false, l'application YouTube est désactivée et son icône est supprimée de l'écran d'accueil.
allowiTunes	Booléen, facultatif. Si cette option est définie sur false, l'iTunes Music Store est désactivé et son icône est supprimée de l'écran d'accueil. L'utilisateur ne peut alors pas prévisualiser, acheter ou télécharger de contenu.
allowSafari	Booléen, facultatif. Si cette option est définie sur false, l'application du navigateur web Safari est désactivée et son icône est supprimée de l'écran d'accueil. Elle empêche également l'utilisateur d'ouvrir des clips web.

Donnée utile LDAP

La donnée utile LDAP est désignée par la valeur PayloadType com.apple.ldap.account . Une relation one-to-many unit le compte LDAP à LDAPSearchSettings. LDAP se présente un peu comme une arborescence. Chaque objet SearchSettings représente un nœud de l'arbre à partir duquel lancer la recherche et indiquer l'étendue de celle-ci (nœud, nœud + subordonnées de niveau 1, nœud + tous les niveaux de subordonnées). En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
LDAPAccountDescription	Chaîne, facultatif. Description du compte.
LDAPAccountHostName	Chaîne, obligatoire. Hôte
LDAPAccountUseSSL	Booléen, obligatoire. Utiliser ou non SSL.
LDAPAccountUserName	Chaîne, facultatif. Nom de l'utilisateur.
LDAPAccountPassword	Chaîne, facultatif. À utiliser uniquement avec des profils chiffrés.
LDAPSearchSettings	Objet conteneur au plus haut niveau. Un compte peut en posséder plusieurs. Pour être utile, le compte doit en inclure au moins un.
LDAPSearchSettingDescription	Chaîne, facultatif. Description de ce réglage de recherche.
LDAPSearchSettingSearchBase	Chaîne, requis. Du point de vue conceptuel, il s'agit du chemin vers le nœud permettant de lancer une recherche sur « ou=people,o=example corp ».
LDAPSearchSettingScope	Chaîne, requis. Définit la récursivité à utiliser lors de la recherche. Peut correspondre à l'une des trois valeurs suivantes : LDAPSearchSettingScopeBase : nœud immédiatement inférieur sur lequel SearchBase pointe LDAPSearchSettingScopeOneLevel : nœud plus ses subordonnées immédiates. LDAPSearchSettingScopeSubtree : nœud plus toutes ses subordonnées quelle que soit leur profondeur.

Donnée utile CalDAV

La donnée utile CalDAV est désignée par la valeur PayloadType com.apple.caldav.account. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
CalDAVAccountDescription	Chaîne, facultatif. Description du compte.
CalDAVHostName	Chaîne, obligatoire. Adresse du serveur.
CalDAVUsername	Chaîne, obligatoire. Nom de l'utilisateur pour l'ouverture de session.
CalDAVPassword	Chaîne, facultatif. Mot de passe de l'utilisateur.

Clé	Valeur
CalDAVUseSSL	Booléen, obligatoire. Utiliser ou non SSL.
CalDAVPort	Nombre, facultatif. Port permettant de se connecter au serveur.
CalDAVPrincipalURL	Chaîne, facultatif. URL de base pointant sur le calendrier de l'utilisateur.

Donnée utile Calendar Subscription

La donnée utile CalSub est désignée par la valeur PayloadType com.apple.subscribed-calendar.account. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
SubCalAccountDescription	Chaîne, facultatif. Description du compte.
SubCalAccountHostName	Chaîne, obligatoire. Adresse du serveur.
SubCalAccountUsername	Chaîne, facultatif. Nom de l'utilisateur pour l'ouverture de session.
SubCalAccountPassword	Chaîne, facultatif. Mot de passe de l'utilisateur.
SubCalAccountUseSSL	Booléen, obligatoire. Utiliser ou non SSL.

Donnée utile SCEP

La donnée utile SCEP (Simple Certificate Enrollment Protocol) est désignée par la valeur PayloadType com.apple.encrypted-profile-service. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
URL	Chaîne, obligatoire.
Name	Chaîne, facultatif. Toute chaîne interprétée par le serveur SCEP. Il peut s'agir, par exemple, d'un nom de domaine tel que exemple.org. Si une autorité de certificat possède plusieurs certificats, il est possible d'utiliser ce champ pour discerner le certificat nécessaire.
Subject	Matrice, facultatif. Représentation d'un nom X.500 par un tableau de valeurs OID-valeur. Par exemple, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, qui peut se traduire de la manière suivante : [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]] Les OID peuvent se représenter sous forme de chiffres associés à des pointillés, avec les raccourcis correspondant à C, L, ST, O, OU, CN (respectivement pour les pays, localité, état, entreprise, département dans l'entreprise, nom commun).
Challenge	Chaîne, facultatif. Secret pré-partagé.
Keysize	Nombre, facultatif. Taille de la clé en bits, à savoir 1024 ou 2048.

Clé	Valeur
Key Type	Chaîne, facultatif. Toujours « RSA» pour le moment.
Key Usage	Nombre, facultatif. Masque binaire indiquant l'utilisation d'une clé. 1 correspond à une signature, 4 à un chiffrement, 5 pour une signature et un chiffrement. Certains CA, comme Windows CA, prennent en charge uniquement le chiffrement ou les signatures, mais pas simultanément.

Clés de dictionnaire SubjectAltName

La donnée utile SCEP peut spécifier un dictionnaire SubjectAltName facultatif qui fournit les valeurs requises par le CA pour l'émission d'un certificat. Vous pouvez spécifier une seule chaîne ou une matrice de chaînes pour chaque clé. Les valeurs que vous spécifiez dépendent du CA que vous utilisez, mais peuvent inclure des valeurs telles que le nom du DNS, l'URL ou l'adresse électronique. Pour obtenir un exemple, consultez la section « Échantillon de réponse du serveur (phase 3) avec spécifications SCEP » à la page 94.

Clés de dictionnaire GetCACaps

Si vous ajoutez un dictionnaire avec la clé GetCACaps, l'appareil utilise les chaînes que vous fournissez comme source d'informations officielle sur les capacités de votre CA. Sinon, l'appareil interroge le CA à la recherche de GetCACaps et utilise la réponse qu'il reçoit. Si le CA ne répond pas, l'appareil envoie par défaut des requêtes GET 3DES et SHA-1.

Donnée utile APN

La donnée utile APN (Access Point Name) est désignée par la valeur PayloadType com.apple.apn.managed. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
DefaultsData	Dictionnaire, obligatoire. Ce dictionnaire contient deux paires clé-valeur.
DefaultsDomainName	Chaîne, obligatoire. La seule valeur autorisée est « com.apple.managedCarrier ».
apns	Matrice, obligatoire. Cette matrice contient un nombre arbitraire de dictionnaires décrivant chacun une configuration APN avec la paire clé-valeur ci-dessous.
apn	Chaîne, obligatoire. Cette chaîne spécifie le nom du point d'accès.
username	Chaîne, obligatoire. Cette chaîne spécifie le nom d'utilisateur de cet APN. Si elle est manquante, l'appareil permet de la saisir pendant l'installation.

Clé	Valeur
password	Données, facultatif. Cette donnée représente le mot de passe de l'utilisateur de cet APN. Celle-ci est chiffrée par mesure de sécurité. Si elle manque dans la donnée utile, l'appareil demande de la saisir pendant l'installation du profil.
proxy	Chaîne, facultatif. Adresse IP ou URL du proxy APN.
proxyPort	Nombre, facultatif. Numéro de port du proxy APN.

Donnée utile Exchange

La donnée utile Exchange est désignée par la valeur PayloadType com.apple.eas.account. Cette donnée utile crée un compte Microsoft Exchange sur l'appareil. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
EmailAddress	Chaîne, obligatoire. Si cette clé n'apparaît pas dans la donnée utile, l'appareil invite à saisir cette chaîne pendant l'installation du profil. Spécifie l'adresse électronique complète du compte.
Host	Chaîne, obligatoire. Spécifie le nom d'hôte (ou l'adresse IP) du serveur Exchange.
SSL	Booléen, facultatif. La valeur par défaut est « YES ». Spécifie si le serveur Exchange utilise SSL pour l'authentification.
UserName	Chaîne, obligatoire. Cette chaîne spécifie le nom d'utilisateur du compte Exchange. Si elle est manquante, l'appareil demande de la saisir pendant l'installation du profil.
Mot de passe	Chaîne, facultatif. Mot de passe du compte. À utiliser uniquement avec des profils chiffrés.
Certificat	Facultatif. Pour les comptes qui permettent l'authentification par certificat, il s'agit d'un certificat d'identité .p12 dans un format blob NSData.
CertificateName	Chaîne, facultatif. Spécifie le nom ou la description du certificat.
CertificatePassword	Facultatif. Mot de passe nécessaire pour le certificat d'identité p12. À utiliser uniquement avec des profils chiffrés.

Donnée utile VPN

La donnée utile VPN est désignée par la valeur PayloadType com.apple.vpn.managed. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
UserDefinedName	Chaîne. Description de la connexion VPN affichée sur l'appareil.
OverridePrimary	Booléen. Spécifie s'il faut envoyer tout le trafic au travers de l'interface VPN. Si la valeur est vraie, l'ensemble du trafic réseau est envoyé par le VPN.
VPNType	Chaîne. Détermine les réglages disponibles dans la donnée utile pour ce type de connexion VPN. Elle peut avoir trois valeurs possibles : « L2TP », « PPTP » ou « IPSec », qui représentent L2TP, PPTP et Cisco IPSec respectivement.

Deux dictionnaires peuvent être présents au niveau le plus élevé, sous les clés « PPP » et « IPSec ». Les clés à l'intérieur de ces deux dictionnaires sont décrites ci-dessous en même temps que la valeur VPNType sous laquelle ces clés sont utilisées.

Clés de dictionnaire PPP

Les éléments suivants sont destinés aux données utiles VPN de type PPP.

Clé	Valeur
AuthName	Chaîne. Nom d'utilisateur du compte VPN. Utilisé pour L2TP et PPTP.
AuthPassword	Chaîne, facultatif. Visible uniquement si TokenCard est faux. Utilisé pour L2TP et PPTP.
TokenCard	Booléen. Spécifie s'il faut utiliser une carte de jeton, comme une carte RSA SecurID, pour la connexion. Utilisé pour L2TP.
CommRemoteAddress	Chaîne. Adresse IP ou nom d'hôte du serveur VPN. Utilisé pour L2TP et PPTP.
AuthEAPPlugins	Matrice. Présente uniquement si RSA SecurID est utilisé, auquel cas elle a une seule entrée, une chaîne avec la valeur « EAP-RSA ». Utilisé pour L2TP et PPTP.
AuthProtocol	Matrice. Présente uniquement si RSA SecurID est utilisé, auquel cas elle a une seule entrée, une chaîne avec la valeur « EAP ». Utilisé pour L2TP et PPTP.
CCPMPPE40Enabled	Booléen. Consultez la description de CCPEnabled. Utilisé pour PPTP.

Clé	Valeur
CCPMPPE128Enabled	Booléen. Consultez la description de CCPEnabled. Utilisé pour PPTP.
CCPEnabled	Booléen. Active le chiffrement sur la connexion. Si cette clé et CCPMPPE40Enabled sont vrais, représente le niveau de chiffrement automatique ; si cette clé et CCPMPPE128Enabled sont vrais, représente le niveau de chiffrement maximum. Si aucun chiffrement n'est utilisé, aucune des clés CCP n'est vraie. Utilisé pour PPTP.

Clés de dictionnaire IPSec

Les éléments suivants sont destinés aux données utiles VPN de type IPSec.

Clé	Valeur
RemoteAddress	Chaîne. Adresse IP ou nom d'hôte du serveur VPN. Utilisé pour Cisco IPSec.
AuthenticationMethod	Chaîne. Soit « SharedSecret » soit « Certificate ». Utilisé pour L2TP et Cisco IPSec.
XAuthName	Chaîne. Nom d'utilisateur du compte VPN. Utilisé pour Cisco IPSec.
XAuthEnabled	Entier. 1 si XAUTH est égal à « ON », 0 s'il est égal à « OFF ». Utilisé pour Cisco IPSec.
LocalIdentifier	Chaîne. Présent uniquement si AuthenticationMethod = SharedSecret. Le nom du groupe à utiliser. En cas d'utilisation de l'authentification hybride, la chaîne doit se terminer par « [hybrid] ». Utilisé pour Cisco IPSec.
LocalIdentifierType	Chaîne. Présent uniquement si AuthenticationMethod = SharedSecret. La valeur est « KeyID ». Utilisé pour L2TP et Cisco IPSec.
SharedSecret	Donnée. Secret partagé du compte VPN. Présent uniquement si AuthenticationMethod = SharedSecret. Utilisé pour L2TP et Cisco IPSec.
PayloadCertificateUUID	Chaîne. UUID du certificat à utiliser pour les références du compte. Présent uniquement si AuthenticationMethod = Certificate. Utilisé pour Cisco IPSec.
PromptForVPNPIN	Booléen. Spécifie s'il faut inviter à saisir un PIN lors de la connexion. Utilisé pour Cisco IPSec.

Donnée utile Wi-Fi

La donnée utile Wi-Fi est désignée par la valeur PayloadType com.apple.wifi.managed. Elle décrit la version 0 de la valeur PayloadVersion. En plus des réglages communs à toutes les données utiles, cette donnée utile définit ce qui suit :

Clé	Valeur
SSID_STR	Chaîne. SSID du réseau Wi-Fi à utilisé.
HIDDEN_NETWORK	Booléen. En plus du SSID, l'appareil utilise des informations comme le type de diffusion et le type de chiffrement pour identifier un réseau. Par défaut, le programme part du principe que tous les réseaux configurés sont ouverts ou diffusent des données. Pour spécifier un réseau masqué, vous devez inclure une valeur booléenne à la clé « HIDDEN_NETWORK ».
EncryptionType	Chaîne. Les valeurs possibles pour « EncryptionType » sont « WEP », « WPA » ou « Any ». « WPA » correspond à WPA et WPA2 et s'applique aux deux types de chiffrement. Assurez-vous que ces valeurs correspondent exactement aux possibilités du point d'accès réseau. Si vous n'êtes pas sûr du type de chiffrement ou préférez que « EncryptionType » s'applique à tous les types de chiffrement, utilisez la valeur « Any ».
Mot de passe	Chaîne, facultatif. L'absence de mot de passe n'empêche pas l'ajouter du réseau à la liste des réseaux connus. L'utilisateur est finalement invité à fournir le mot de passe à la connexion à ce réseau.

Pour les réseaux d'entreprise 802.1X, le dictionnaire de configuration de client EAP doit être fourni.

Dictionnaire EAPClientConfiguration

En plus des types de chiffrement standard, il est possible de spécifier un profil d'entreprise pour un réseau donné par le biais de la clé « EAPClientConfiguration ». S'il est présent, sa valeur est un dictionnaire avec les clés suivantes.

Clé	Valeur
UserName	Chaîne, facultatif. À moins que vous ne connaissiez le nom d'utilisateur exact, cette propriété n'apparaîtra pas dans une configuration importée. Les utilisateurs peuvent saisir cette information à l'authentification.
AcceptEAPTypes	Matrice de nombres entiers. Les types d'EAP suivants sont acceptés : 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST

Clé	Valeur
PayloadCertificateAnchorUUID	Matrice de chaînes, facultative. Identifie les certificats auxquels il faut faire confiance pour cette authentification. Chaque entrée doit contenir l'UUID de la donnée utile de certificat. Utilisez cette clé pour empêcher l'appareil de demander à l'utilisateur si les certificats présents dans la liste sont fiables. La confiance dynamique (la zone de dialogue du certificat) est désactivée si cette propriété est spécifiée, à moins que TLSAllowTrustExceptions soit également spécifié avec la valeur vrai plus bas.
TLSTrustedServerNames	Matrice de chaînes, facultatif. Il s'agit de la liste des noms usuels des certificats de serveur qui seront acceptés. Vous pouvez utiliser des caractères de remplacement pour spécifier un nom, comme wpa.*.example.com. Si un serveur présente un certificat qui ne figure pas dans cette liste, le certificat n'est pas considéré comme fiable. Utilisée seule ou associée à TLSTrustedCertificates, cette propriété permet de définir finement les certificats de confiance pour le réseau en question et d'éviter l'usage de certificats auxquels la confiance est accordée de manière dynamique. La confiance dynamique (la zone de dialogue du certificat) est désactivée si cette propriété est spécifiée, à moins que TLSAllowTrustExceptions soit également spécifié avec la valeur vrai plus bas.
TLSAllowTrustExceptions	Booléen, facultatif. Autorise/refuse la prise d'une décision de confiance dynamique par l'utilisateur. La confiance dynamique est la zone de dialogue de certificat qui apparaît lorsqu'il n'est pas fait confiance à un certificat. Si cette clé est fausse, l'authentification échoue s'il n'est pas encore fait confiance au certificat. Consultez PayloadCertificateAnchorUUID et TLSTrustedNames ci-avant. La valeur par défaut de cette propriété est vrai à moins que PayloadCertificateAnchorUUID ou TLSTrustedServerNames ne soient fournis, auquel cas la valeur par défaut est faux.
TTLSInnerAuthentication	Chaîne, facultatif. Authentification interne utilisée par le module TTLS. La valeur par défaut est « MSCHAPv2 ». Les valeurs possibles sont « PAP », « CHAP », « MSCHAP » et « MSCHAPv2 ».
OuterIdentity	Chaîne, facultatif. Cette clé n'a d'importance que pour TTLS, PEAP et EAP-FAST. Elle permet à l'utilisateur de masquer son identité. Le nom réel de l'utilisateur n'apparaît que dans le tunnel chiffré. Par exemple, il peut être défini sur « anonymous », « anon » ou « anon@mon_entreprise.net ». Elle permet d'améliorer la sécurité parce qu'un attaquant ne voit pas apparaître le nom de l'utilisateur qui s'authentifie en clair.

Prise en charge d'EAP-Fast

Le module EAP-FAST utilise les propriétés suivantes dans le dictionnaire EAPClientConfiguration.

Clé	Valeur
EAPFASTUsePAC	Booléen, facultatif.
EAPFASTProvisionPAC	Booléen, facultatif.
EAPFASTProvisionPACAnonymously	Booléen, facultatif.

Ces clés sont de nature hiérarchique : si EAPFASTUsePAC est fausse, les deux autres propriétés ne sont pas consultées. De même, si EAPFASTProvisionPAC est fausse, EAPFASTProvisionPACAnonymously n'est pas consultée.

Si EAPFASTUsePAC est fausse, l"authentification se poursuit un peu comme pour PEAP ou TTLS : le serveur prouve chaque fois son identité à l'aide d'un certificat.

Si la valeur d'EAPFASTUsePAC est vraie, un PAC existant est utilisé s'il est présent. La seule manière d'obtenir un PAC sur l'appareil à ce jour consiste à autoriser l'approvisionnement de PAC. Vous devez donc activer EAPFASTProvisionPAC et, si vous le souhaitez, EAPFASTProvisionPACAnonymously. EAPFASTProvisionPACAnonymously a une faiblesse de sécurité : il n'authentifie pas le serveur, les connexions sont donc vulnérables aux attaques de type homme du milieu (MITM).

Certificats

Comme pour les configurations VPN, il est possible d'associer une configuration d'identité de certificat à une configuration Wi-Fi. Cela s'avère pratique lors de la définition de références pour un réseau d'entreprise. Pour associer une identité, spécifiez l'UUID de sa donnée utile via la clé « PayloadCertificateUUID ».

Clé	Valeur
PayloadCertificateUUID	Chaîne. UUID de la donnée utile de certificat à utiliser pour les références de l'identité.

Profils de configuration d'échantillon

Cette section inclut des profils exemples qui illustrent les phases d'inscription et de configuration en mode OTA. Voici quelques extraits, les besoins variant en fonction des exemples. Pour une aide sur la syntaxe, consultez les détails fournis plus haut dans cette annexe. Pour une description de chaque phase, consultez « Inscription et configuration en mode OTA » à la page 24.

Échantillon de réponse du serveur (phase 1)

```
<?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>PRODUIT</string>
        </array>
    <key>Challenge</key>
     <string>challenge facultatif</string>
     ou
     <data>base64-encoded</data>
    </dict>
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string>Service de profils</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>Saisissez l'appareil dans le service de profil chiffré Example
     Inc</string>
    <key>PayloadType</key>
     <string>Service de profils</string>
</dict>
</plist>
```

Échantillon de réponse de l'appareil (phase 2)

```
<?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>
soit :
    <string>Chaîne</string>
soit :
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

Échantillon de réponse du serveur (phase 3) avec spécifications SCEP

```
<?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>Fournit l'identité de chiffrement de l'appareil</string>
          <key>PayloadUUID</key>
          <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
          <key>PayloadType</key>
          <string>com.apple.security.scep</string>
          <key>PayloadDisplayName</key>
          <string>Identité de chiffrement</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>
```

Échantillon de réponse de l'appareil (phase 4)

```
<?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>
```

Exemples de scripts

Cette annexe fournit des exemples de scripts pour les tâches de déploiement de l'iPhone OS.

Les scripts de cette section doivent être modifiés pour être adaptés à vos besoins et à vos configurations.

Exemple de script C# pour « Utilitaire de configuration iPhone »

Cet exemple de script montre comment créer des fichiers de configuration à l'aide d'« Utilitaire de configuration iPhone » pour Windows.

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

public class TestScript : IScript
  {
  private IApplication _host;

  public TestScript()
     {
     }

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    }
}
```

Exemple d'AppleScript pour « Utilitaire de configuration iPhone »

Cet exemple de script montre comment créer des fichiers de configuration à l'aide d'« Utilitaire de configuration iPhone » pour Mac OS X.

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