



iPhone dans l'entreprise

Règlements Exchange ActiveSync pris en charge

Les stratégies Exchange suivantes sont prises en charge :

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

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

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

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

Les utilisateurs peuvent également réinitialiser un de leurs appareils en choisissant « Effacer contenu et réglages » dans le menu Réinitialiser des Réglages généraux. Vous

Fonctionnalités ActiveSync Exchange complémentaires prises en charge

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

- la création d'invitations à des événements en calendrier (grâce à Microsoft Exchange

'iPhoneets li o ouch prennent en charge lses normses de s.2frité de mris en réseau()] TJ ETBT 10 0

Comptes de messagerie

Réseaux privés virtuels

L'accès sécurisé à des réseaux privés est pris en charge sur l'iPhone et l'iPod touch 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 infrastru32 vir.

Phase 3 – Installation du certificat : en étape 1, le service de profils répond avec les instructions pour que l'appareil génère une clé (RSA 1024) et 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 88.

Phase 4 – Configuration de l'appareil :

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/>

Création et déploiement de profils de configuration

2

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

La barre latérale contient également **Appareils**, qui affiche des informations sur l'iPhone ou l'iPod touch connecté au port USB de votre ordinateur. Des informations relatives à l'appareil branché s'ajoutent automatiquement à la liste **Appareils** afin que vous puissiez les consulter à nouveau sans avoir à reconnecter l'appareil. Après qu'un appareil ait été branché, vous pouvez également chiffrer les données de l'appareil.

Lorsque qu'un appareil est branché, vous avez la possibilité de passer par **Utilitaires**

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 don-

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

Réglages « Calendriers auxquels vous êtes abonné »

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

Installation par les utilisateurs de profils de configuration téléchargés
Fournissez à vos utilisateurs l'URL à laquelle ils peuvent télécharger les profils sur leur

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

Réglages PPTP

Lorsque vous configurez l'appareil manuellement pour un VPN PPTP, un écran sembla-

Réglages L2TP

Réglages Wi-Fi

Pour modifier des réglages Wi-Fi, allez à Réglages > Général > Réseau > Wi-Fi.

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 sur l'écran Mot de passe pour le certificat ou une identité. 0 10 174 677.333Tm /F1.042Tm F2.Configuration

L'on utilise iTunes pour synchroniser de la musique et de

Mise à jour manuelle

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

buer iTunes à vos utilisateurs.

Vous pouvez distribuer des applications iPhone et iPod touch 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 et l'iPod touch. Si vous développez une application, vous pouvez la distribuer à l'aide d'iTunes.

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

Mettez les instructions suivantes pour configurer votre serveur VPN Cisco pour pouvoir l'utiliser avec l'iPhone et l'iPod touch.

Plate-formes Cisco prises en charge

iPhone 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 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.

fil, comme « com.mon_entreprise.iPhone.reglages_courrier » ou

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.

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 :

Type de clé
Key Usage

Chaîne, facultatif. Toujours « RSA » pour le moment.
Nombre, facultatif. Masque de bit qui indique l'usage pour la clé.

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 :

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 :

Deux dictionnaires peuvent être présents au niveau le plus élevé, sous les clés « PPP »


```
<string>Apple Inc.</string>  
</array>
```

