Déploiement de Windows Mobile® 6 avec Windows® Essential Business Server 2008

Microsoft® Corporation

Date de publication : Octobre 2008

Résumé

Ce document fournit les étapes et les instructions à suivre pour déployer des appareils fonctionnant sous Windows Mobile® 6 dans une infrastructure informatique basée sur la solution serveur Windows® Essential Business Server 2008 (Windows EBS 2008).

Les informations contenues dans ce document représentent l'opinion actuelle de Microsoft Corporation sur les points cités à la date de publication. Microsoft s'adapte aux conditions fluctuantes du marché et cette opinion ne doit pas être interprétée comme un engagement de la part de Microsoft. De plus, Microsoft ne peut pas garantir la véracité de toute information présentée après la date de publication.

Ce livre blanc est fourni uniquement à titre indicatif. MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE, IMPLICITE OU STATUTAIRE, EN CE QUI CONCERNE CE DOCUMENT.

L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans la permission expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur tout ou partie des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Sauf indication contraire, les sociétés, organisations, produits, noms de domaine, adresses électroniques, logos, personnes, lieux et événements utilisés dans les exemples sont fictifs. Toute ressemblance avec des sociétés, organisations, produits, noms de domaine, adresses électroniques, logos, personnes, lieux et événements réels est purement fortuite et involontaire.

© 2008 Microsoft Corporation. Tous droits réservés.

Microsoft, ActiveSync, Excel, Outlook, PowerPoint, SharePoint, Windows, Windows Live, Windows Mobile, Windows Server et Windows Vista sont soit des marques de Microsoft Corporation, soit des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

UPnP est une marque d'homologation d'UPnP Implementers Corporation.

Toutes les autres marques appartiennent à leurs propriétaires respectifs.

Table des matières

Déploiement de Windows Mobile 6 avec Windows Essential Business Server 2008 5
Windows Mobile 6 5
Windows Mobile 6.1 6
Avant de commencer 7
Niveau de compétences requis 7
Configuration requise pour Windows Mobile 7
Configuration serveur requise 8
Étapes du processus de déploiement 8
Étape 1 : Installation de Microsoft ActiveSync 4.5 ou WMDC 6.1 9
Étape 2 : Activation des services mobiles pour les utilisateurs 10
Étape 3 : Configuration du pare-feu et des services Web 12
Étape 4 : Installation et configuration d'un certificat 14
Choix du type de certificat 14
Configuration d'un certificat 16
Option A : Utilisation d'un certificat auto-émis 16
Option B : Utilisation d'un certificat tiers 19
Étape 5 : Installation et configuration du certificat tiers sur le serveur d'administration de la sécurité 23
Étape 6 : Configuration du serveur de messagerie Windows Essential Business Server 2008 25
Vérification du démarrage du service de site 25
Étape 7 : Configuration de la synchronisation de l'appareil 25
Option A : Synchronisation OTA de l'appareil 25
Option B : Synchronisation de l'appareil à l'aide d'ActiveSync 28
Synchronisation de l'appareil à l'aide du Gestionnaire pour appareils Windows Mobile (WMDC) 30
Étape 8 : Test du déploiement 36
Test de la synchronisation OTA 36
Test de la technologie Direct Push 37
Gestion à distance 37
Effacement à distance des données de l'appareil 37
Règles de sécurité de l'appareil 39
Conclusion 41

Résolution des problèmes 41
Installation de Microsoft ActiveSync sur les ordinateurs clients 41
Configuration d'ActiveSync 42
Synchronisation de l'appareil mobile 44
Certains utilisateurs ne peuvent pas synchroniser 44
Aucun utilisateur ne peut synchroniser 44
Déploiement des certificats 46
Obtention d'un certificat 46
Création d'une demande de signature de certificat 47
Installation d'un certificat auto-émis 47
Configuration de l'appareil 47
Messages Direct Push 47
Stratégie de l'appareil 47
Synchronisation 48
Liens connexes 48

Déploiement de Windows Mobile 6 avec Windows Essential Business Server 2008

Windows® Essential Business Server 2008 (EBS 2008) est une nouvelle solution d'infrastructure répartie sur trois serveurs indépendants. Cette solution offre aux entreprises de taille moyenne des fonctionnalités de gestion efficace pour leurs activités quotidiennes, une solution complète de protection des données et des réseaux, un système simplifié de configuration des appareils et des capacités de productivité considérables au sein de l'environnement à haute performance Windows Server®. Grâce au déploiement des appareils Windows Mobile 6 avec EBS 2008, vos employés (le personnel commercial ou mobile) peuvent accéder à leur messagerie, à leurs listes de contacts, à leur calendrier et aux documents stockés sur le site Web de leur société à partir des appareils Windows Mobile 6. Vous pouvez administrer les appareils mobiles comme s'ils étaient installés sur un réseau local. Il vous suffit d'installer des certificats ou d'effacer à distance les données des appareils à des fins de sécurité. EBS 2008 propose une console de gestion simple, sécurisée et consolidée par le biais de laquelle les administrateurs peuvent contrôler les serveurs. Grâce à EBS 2008, vous garantissez la sécurité des accès à partir des appareils mobiles déployés sur votre réseau.

Windows Mobile 6

Windows Mobile 6 est le successeur de Windows Mobile 5.0. Windows Mobile 6 fournit de nouvelles fonctionnalités et de nouveaux outils permettant d'améliorer la productivité, la connectivité et la sécurité. Voici quelques-unes de ses nouvelles fonctionnalités :

- La possibilité d'afficher les messages électroniques au format RTF, avec un accès aux liens directs vers Microsoft® Office SharePoint® ou d'autres sites Web.
- Windows Live™ pour les appareils mobiles, qui permet d'accéder à une variété de services tels que Live Messenger, avec la possibilité de converser avec plusieurs personnes simultanément, d'envoyer des images ou des fichiers et d'enregistrer ou d'envoyer des messages vocaux.
- Les dernières versions mobiles de Microsoft Office, notamment Microsoft Office Outlook® Mobile, Microsoft Office Excel® Mobile et Microsoft Office PowerPoint® Mobile.
- Une interface utilisateur nouvelle et améliorée.

Windows Mobile 6 offre les fonctionnalités suivantes :

- **Technologie Direct Push :** les éléments reçus sur le serveur Microsoft Exchange, à savoir les nouveaux messages électroniques, les modifications des éléments de calendrier ou de contacts ou les mises à jour de tâches, sont immédiatement envoyés vers un appareil exécutant Windows Mobile 6. La technologie Direct Push utilise une connexion Internet basée sur IP et non le service de messages courts (SMS, Short Message Service). L'ancien processus de synchronisation permanente (AUTD, Always-up-to-date) utilise, lui, le service SMS.
- **Communication sans fil pour les informations de contact :** cette fonctionnalité permet de consulter, via une communication sans fil (OTA, over-the-air) des informations contenues dans la liste d'adresses globale stockée sur Microsoft Exchange Server.
- **Règles de sécurité appliquées à distance :** vous pouvez, à distance, gérer et appliquer les paramètres de sécurité sur les appareils mobiles OTA.
- **Effacement local des données de l'appareil :** cette fonctionnalité permet de réinitialiser l'appareil après un certain nombre de tentatives de connexion erronées.
- **Effacement à distance des données de l'appareil :** cette fonctionnalité permet aux administrateurs de réinitialiser un appareil Windows Mobile 6 à distance.

Windows Mobile 6.1

Windows Mobile 6.1, qui succède à la version Windows Mobile 6, inclut des fonctionnalités améliorées pour la configuration de votre téléphone, la gestion des SMS et la vérification des messages électroniques. Windows Mobile 6.1 contient des fonctionnalités qui facilitent la navigation et vous permettent ainsi de gagner du temps. Les utilisateurs peuvent baliser, supprimer ou déplacer des groupes de messages et effectuer le suivi de leurs conversations grâce aux thèmes de discussion. Windows Mobile 6.1 offre aux professionnels plus de gages de sécurité pour leur téléphone Windows Mobile grâce à la mise en place de stratégies mobiles avancées qui permettent aux entreprises de gérer et d'administrer la sécurité des téléphones.

Microsoft Exchange Server 2007 contient un nouveau service de découverte automatique appelé Autodiscover, qui est pris en charge par les appareils Windows Mobile 6.1. Ce service permet aux administrateurs de configurer automatiquement ces appareils une fois que l'utilisateur se connecte à sa messagerie.

Avant de commencer

Niveau de compétences requis

Le présent document s'adresse aux administrateurs d'entreprises de taille moyenne. Pour pouvoir suivre les instructions présentées dans ce document, vous devez maîtriser Exchange Server 2007 et posséder des connaissances de base de Windows Mobile.

Configuration requise pour Windows Mobile

Pour pouvoir déployer une solution de messagerie Windows Mobile 6 dans un environnement Windows Essential Business Server 2008, votre configuration doit répondre aux conditions requises indiquées dans le Tableau 1.

Tableau 1 : Configuration requise pour les appareils mobiles

Configuration requise	Description
Appareil Windows Mobile	Appareil mobile équipé de Windows Mobile 6 ou Windows Mobile 6.1.
Accès Internet	L'appareil mobile doit disposer d'un accès Internet. La connectivité des données peut être établie selon l'une des méthodes suivantes : • GPRS • Accès réseau sans fil
Microsoft ActiveSync® 4.5 (pour Windows XP) Gestionnaire pour appareils Windows Mobile 6.1 (pour Windows Vista)	Microsoft ActiveSync ou le Gestionnaire pour appareils Windows Mobile (WMDC, Windows Mobile Device Center) est l'outil client requis pour synchroniser un appareil Windows Mobile avec l'ordinateur client ou configurer cet appareil avec Exchange Server sur le réseau. Vous pouvez télécharger Microsoft ActiveSync 4.5 à l'adresse suivante : Microsoft Web site (http://www.microsoft.com/france/windowsmobile/articles/activesync45.mspx). Le Gestionnaire pour appareils Windows Mobile est intégré dans Windows Vista et mis à jour via Windows Update. Si l'ordinateur client ne dispose pas de la dernière version du Gestionnaire pour appareils Windows Mobile, vous pouvez télécharger la version 6.1 à l'adresse suivante : Microsoft Web site (http://www.microsoft.com/downloads/results.aspx?pocId=&freetext=Windows%20Mobile%20Device%20Center%206.1&DisplayLang=fr)

Configuration serveur requise

En plus de la configuration requise pour Windows Mobile, assurez-vous de disposer des logiciels serveurs suivants.

Tableau 2 : Configuration serveur requise

Configuration requise	Description
Windows Essential Business Server 2008	Consiste en trois rôles serveurs qui nécessitent l'installation de trois serveurs avec Windows EBS 2008 : serveur d'administration, serveur d'administration de la sécurité et serveur de messagerie.
Certificat tiers approuvé ou certificat auto-émis	Un certificat approuvé par une autorité de certification est requis pour valider la session entre la messagerie installée sur Windows EBS 2008 et l'appareil Windows Mobile. Nous recommandons d'utiliser un certificat tiers. Si vous avez l'intention d'utiliser un certificat auto-émis, suivez les instructions d'installation des certificats auto-émis Windows EBS 2008 sur des appareils Windows Mobile fournies dans ce livre blanc.

Étapes du processus de déploiement

Pour déployer un appareil mobile sur votre réseau Windows EBS 2008, procédez comme suit :

- Étape 1 : Installation de Microsoft ActiveSync 4.5 ou WMDC 6.1
- Étape 2 : Activation des services mobiles pour les utilisateurs
- Étape 3 : Configuration du pare-feu et des services Web
- Étape 4 : Installation et configuration d'un certificat
- Étape 5 : Installation et configuration du certificat tiers sur le serveur d'administration de la sécurité
- Étape 6 : Configuration du serveur de messagerie Windows Essential Business Server 2008
- Étape 7 : Configuration de la synchronisation de l'appareil
- Étape 8 : Test du déploiement

Étape 1 : Installation de Microsoft ActiveSync 4.5 ou WMDC 6.1

Les appareils Windows Mobile peuvent être configurés pour effectuer une synchronisation OTA avec Exchange Server sous Windows Essential Business Server 2008. L'appareil doit dans ce cas faire l'objet d'un plan de données. L'utilisateur doit disposer des informations requises pour pouvoir configurer l'appareil afin qu'il se connecte à Exchange Server, à savoir l'adresse Exchange Server, le nom d'utilisateur, le mot de passe et le nom de domaine. Les instructions de configuration de la synchronisation doivent être appliquées lorsque le serveur est configuré pour un accès sans fil à l'appareil Windows Mobile. Ces instructions sont fournies à l'**Étape 7 : Configuration de la synchronisation de l'appareil**. Vous pouvez également connecter les appareils mobiles à un ordinateur client pour copier des fichiers, installer des applications et synchroniser des données directement avec l'ordinateur. Pour pouvoir connecter un appareil mobile à un ordinateur client, vous devez installer ActiveSync 4.5 sur les ordinateurs clients fonctionnant sous Windows XP ou le Gestionnaire pour appareils Windows Mobile (WMDC) pour les ordinateurs clients fonctionnant sous Windows Vista.

Installez manuellement Microsoft ActiveSync 4.5 ou WMDC sur les ordinateurs clients qui seront connectés à un appareil Windows Mobile. Copiez le fichier d'installation sur chaque ordinateur client et exécutez le programme d'installation.

Remarque

Vous pouvez télécharger le fichier d'installation de Microsoft ActiveSync 4.5 pour les ordinateurs fonctionnant sous Windows XP à l'adresse suivante : Microsoft Web site (http://www.microsoft.com/france/windowsmobile/articles/activesync45.mspx).

Avant d'installer ActiveSync 4.5 sur un ordinateur, vérifiez que celui-ci dispose de la configuration système minimale requise pour Microsoft ActiveSync 4.5, à l'adresse suivante : Microsoft Web site (http://www.microsoft.com/france/windowsmobile/articles/activesync45.mspx).

Remarque

Le Gestionnaire pour appareils Windows Mobile est intégré dans Windows Vista et mis à jour via Windows Update. Si l'ordinateur client ne dispose pas de la dernière version du Gestionnaire pour appareils Windows Mobile, vous pouvez télécharger la version 6.1 à l'adresse suivante : Microsoft Web site (http://www.microsoft.com/france/windowsmobile/devicecenter.mspx)

Étape 2 : Activation des services mobiles pour les utilisateurs

Les comptes d'utilisateur nouvellement créés dans Windows EBS 2008 disposent par défaut des services mobiles tels qu'Outlook Web Access et Exchange ActiveSync.

Pour vérifier si les services mobiles Outlook Web Access et Exchange ActiveSync sont activés pour un utilisateur, suivez les étapes ci-dessous :

Vous devez au préalable vous connecter à la console de gestion Exchange sur le serveur de messagerie via la console d'administration.

1. Démarrez la console d'administration. Pour cela, cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sélectionnez **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques (Computers and Devices)**. Sélectionnez le serveur de messagerie dans la liste des serveurs, puis cliquez sur **Exchange Management Console** dans le volet Tâches (Tasks) du serveur de messagerie.
3. Cliquez sur le bouton **Connexion (Connect)**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de messagerie. Cliquez sur **OK**.
4. Dans l'arborescence de la console de gestion Exchange, développez **Configuration du destinataire (Recipient Configuration)**, puis sélectionnez **Boîte aux lettres (Mailbox)**.
5. Double-cliquez sur le nom complet de l'utilisateur qui s'affiche dans le volet des résultats pour ouvrir la boîte de dialogue des propriétés.
6. Cliquez sur l'onglet **Fonctionnalités de boîte aux lettres (Mailbox Features)**. Vérifiez l'indicateur d'état d'**Outlook Web Access** et d'**Exchange ActiveSync**. S'il est désactivé, sélectionnez la fonctionnalité, puis cliquez sur **Activer (Enable)**.

Remarque

La fonctionnalité Outlook Web Access ne doit pas nécessairement être activée pour que l'appareil Windows Mobile puisse accéder à une boîte aux lettres Exchange. Cette fonctionnalité permettra toutefois de régler les problèmes de connectivité.

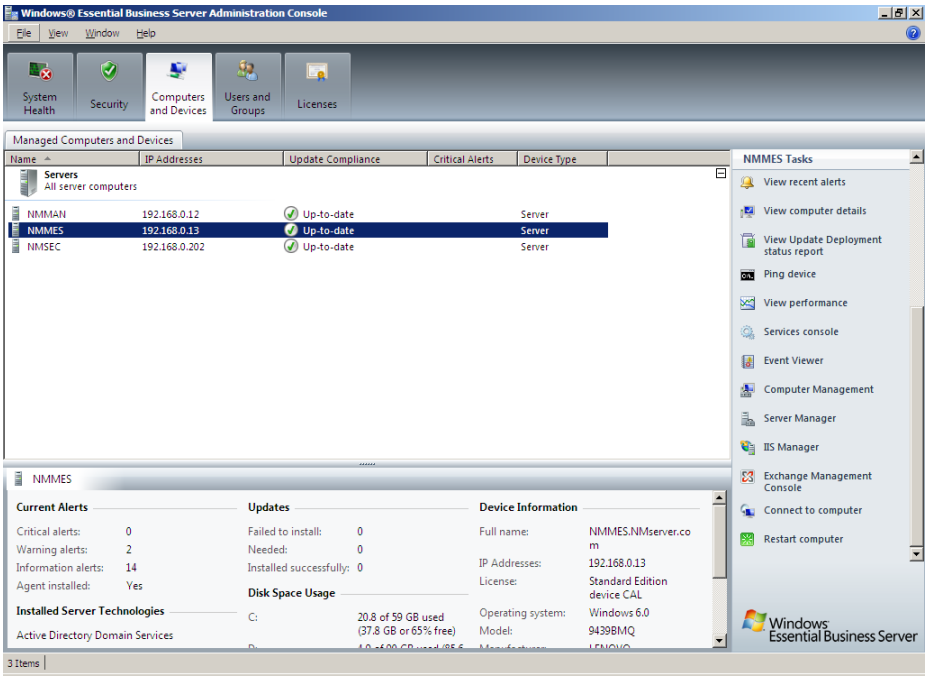

Figure 1 : Accès à la console de gestion Exchange du serveur de messagerie via la Console d'administration de Windows Essential Business Server

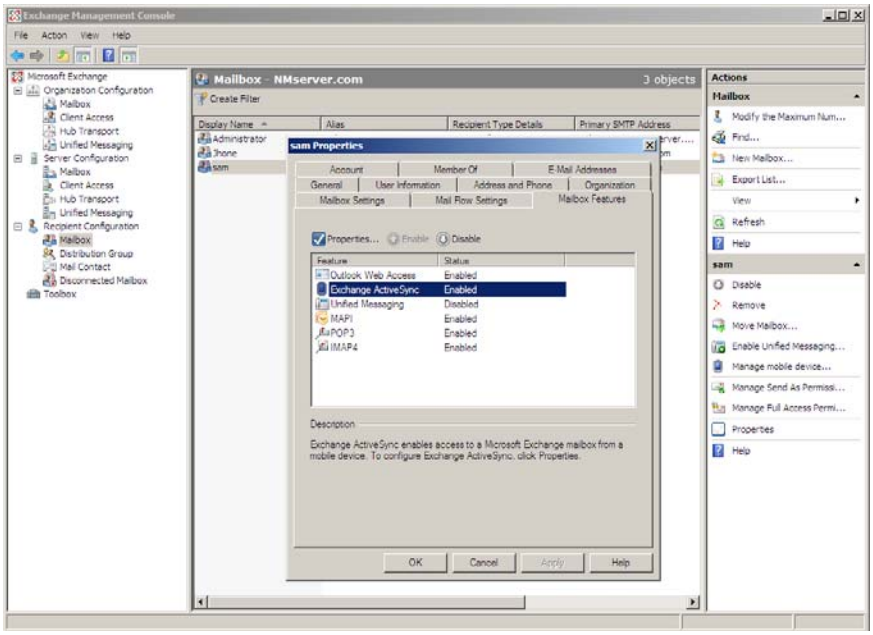

Figure 2 : Vérification de l'activation de la fonctionnalité Exchange ActiveSync dans Fonctionnalités de boîte aux lettres (Mailbox Features)

Remarque

Technologie Direct Push

La technologie Direct Push permet aux utilisateurs d'accéder immédiatement aux nouvelles informations ou modifications d'informations stockées sur le serveur Exchange, notamment les messages électroniques, les éléments de calendrier et de contact et les tâches. Exchange ActiveSync, qui utilise la technologie Direct Push, actualise les données des appareils mobiles avec celles de la boîte aux lettres Exchange de l'utilisateur. Direct Push fonctionne uniquement via une connexion HTTPS. Exchange ActiveSync est activé par défaut.

Étape 3 : Configuration du pare-feu et des services Web

La solution de pare-feu utilisée dans le réseau Windows EBS 2008 doit être configurée pour autoriser et rediriger les connexions entrantes HTTP sécurisées (HTTPS) vers le serveur de messagerie. Cette solution permet aux appareils mobiles d'accéder aux informations stockées sur Microsoft Exchange Server par synchronisation OTA via Exchange ActiveSync.

Le trafic HTTPS est activé par défaut sur le serveur d'administration de la sécurité, dans la règle de pare-feu de Microsoft Forefront Threat Management Gateway.

Si votre réseau contient un pare-feu logiciel/matériel tiers, vous devez le configurer pour qu'il dirige le trafic HTTPS (pour l'accès aux boîtes aux lettres du serveur de messagerie) vers le serveur d'administration de la sécurité dans le réseau Windows EBS 2008.

Si vous utilisez un pare-feu qui ne prend pas en charge la technologie UPnP, vous devez le configurer manuellement pour qu'il dirige le trafic entrant sur le Port TCP 443 vers l'adresse IP du serveur exécutant Windows EBS 2008.

Assurez-vous d'accorder les privilèges d'accès aux utilisateurs appropriés dans la stratégie de pare-feu logiciel/matériel tiers de façon à ce que seuls les utilisateurs autorisés puissent accéder à Internet via le pare-feu.

Remarque

Les versions Standard et Premium de Windows Essential Business Server 2008 ne contiennent pas Microsoft Internet Security and Acceleration (ISA) Server.

Les éditions Windows EBS 2008 contiennent Microsoft Forefront Threat Management Gateway sur le serveur d'administration de la sécurité. Forefront Threat Management Gateway (TMG) correspond à la prochaine version de Microsoft ISA Server, avec de nouvelles fonctionnalités et technologies de sécurité.

Par défaut, la stratégie de pare-feu de Forefront TMG autorise la communication sur le port 443 (pour le trafic HTTPS).

Pour vérifier si la stratégie de pare-feu est configurée pour autoriser le trafic HTTPS sur le serveur d'administration de la sécurité Windows EBS 2008, suivez les étapes ci-dessous :

Vous devez au préalable vous connecter à la console de gestion Exchange sur le serveur d'administration de la sécurité via la console d'administration.

1. Démarrez la console d'administration. Pour cela, cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sélectionnez **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur d'administration de la sécurité dans la liste des serveurs, puis cliquez sur **Console de Forefront threat Management Gateway** dans le volet Tâches du serveur de messagerie.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur d'administration de la sécurité. Cliquez sur **OK**.
4. Dans l'arborescence de la console de Microsoft Forefront Threat Management Gateway, développez **Stratégie de pare-feu**.
5. Assurez-vous que les stratégies de pare-feu **Publication Microsoft Exchange Server : Outlook Web Access** et **Règles de publication Web de Microsoft Exchange ActiveSync** sont activées. Pour cela, vérifiez les valeurs Action et Protocoles et modifiez-les si nécessaire pour qu'elles affichent « Autoriser » et « HTTPS ».

Pour plus d'informations sur la configuration par défaut des règles de stratégie de Microsoft Forefront Threat Management Gateway (TMG) dans Windows EBS, consultez l'adresse Microsoft Web site. (http://technet.microsoft.com/en-us/library/cc940975.aspx)

Étape 4 : Installation et configuration d'un certificat

Cette section permet de vous guider dans le choix et la configuration d'un certificat. Un certificat permet de synchroniser des données en toute sécurité à l'aide du protocole SSL (Secure Sockets Layer). Il est important d'utiliser ce type de protocole afin de sécuriser les communications entre l'appareil mobile et le serveur.

Choix du type de certificat

Vous pouvez choisir l'un des deux types de certificats suivants :

- **Certificat tiers (recommandé) :** vous pouvez acheter et installer un certificat émis par une autorité de certification principale de confiance approuvée. Les appareils Windows Mobile 6 sont livrés avec une variété de certificats principaux de confiance émis par les principaux fournisseurs de certificats qui sont répertoriés dans le magasin de certificats de l'appareil.

  L'utilisation d'un certificat tiers approuvé est préférable à l'utilisation d'un certificat auto-émis et ce afin de réduire la charge de gestion des certificats. Cependant, vous pouvez utiliser un certificat auto-émis s'il est impossible d'utiliser un certificat tiers.
- **Certificat auto-émis :** vous pouvez utiliser le certificat auto-émis généré par Windows Essential Business Server 2008. Cependant, ce type de certificat doit être distribué aux utilisateurs en vue d'une installation sur leurs ordinateurs et appareils mobiles. Les ordinateurs faisant partie d'un domaine reçoivent le certificat automatiquement. En revanche, le certificat doit être installé manuellement sur l'appareil et les ordinateurs qui ne font pas partie d'un domaine. Si votre organisation envisage de fournir un accès interne aux utilisateurs qui se trouvent à l'extérieur du domaine, un certificat tiers approuvé est recommandé.

Remarque

Windows Mobile 6 propose deux magasins de certificats :

- Le magasin de l'appareil contenant tous les certificats principaux installés par le fabricant.
- Le magasin de l'utilisateur dans lequel des certificats supplémentaires sont enregistrés. Les certificats auto-émis générés par Windows EBS 2008 sont enregistrés dans le magasin d'utilisateurs.

Le tableau suivant présente les avantages et inconvénients de l'utilisation de ces deux types de certificats sur les appareils Windows Mobile. Choisissez le type de certificat le mieux adapté à votre environnement.

Tableau 3 : Avantages et inconvénients des certificats tiers et des certificats auto-émis

Type de certificat	Avantages	Inconvénients
Certificat tiers	• Aucune configuration supplémentaire n'est requise pour les appareils Windows Mobile. • Peut être utilisé avec tous les appareils Windows Mobile Classic, Professional et Standard. • Offre des avantages supplémentaires avec d'autres fonctionnalités de Windows EBS, telles qu'Outlook Web Access, le Poste de travail Web à distance et Outlook Anywhere (RPC sur HTTP).	• Doit être acheté et peut impliquer des frais récurrents pour chaque renouvellement. Peut coûter environ entre 25 et 1 000 euros par an. • Ne peut pas être installé immédiatement. Les informations sur votre société doivent être vérifiées de façon indépendante avant l'émission du certificat. En revanche, il existe certains certificats tiers pouvant être installés immédiatement, mais ce sont des exceptions.
Certificat auto-émis généré par Windows Essential Business Server	• Généré automatiquement par Windows EBS lors de l'installation. • Aucuns frais supplémentaires. • Très peu de configurations sont nécessaires dans Windows EBS 2008.	• Requiert une configuration supplémentaire sur l'appareil. Le certificat doit être installé sur chaque appareil. • Le certificat doit être renouvelé au bout de 5 ans.

Un certificat tiers offre d'autres avantages pratiques aux utilisateurs d'un réseau Windows EBS 2008. Par exemple, ils peuvent utiliser Outlook Anywhere, Outlook Web Access, le Poste de travail Web à distance, Microsoft Windows SharePoint® Services ou d'autres sites Web sécurisés hébergés sur le serveur Windows EBS 2008.

Configuration d'un certificat

En fonction du type de certificat sélectionné, vous devez implémenter les éléments suivants pour que la synchronisation Exchange ActiveSync s'effectue correctement :

a. Procurez-vous un certificat tiers ou faites une demande de signature de certificat pour l'obtenir. Il est inutile d'installer le certificat tiers sur les appareils Windows Mobile 6 puisqu'ils offrent déjà une variété de certificats approuvés. Dans le cas d'un certificat auto-émis, le serveur de messagerie Windows EBS 2008 et le serveur d'administration de la sécurité utilisent le certificat auto-émis par défaut généré par l'autorité de certification privée de Windows EBS 2008. Dans la mesure où le certificat auto-émis ne figure pas dans le magasin de certificats Windows Mobile, vous devez l'installer manuellement sur l'appareil mobile.

b. Exportez et installez un certificat tiers approuvé dans le magasin de certificats du serveur d'administration de la sécurité de Windows EBS 2008. Dans le cas d'un certificat auto-émis généré par Windows EBS 2008, le serveur d'administration de la sécurité utilise ce certificat par défaut, sans aucune installation.

c. Assignez le certificat tiers approuvé au port d'écoute Web externe de Microsoft TMG (sur le serveur d'administration de la sécurité). Par défaut, le port d'écoute Web externe est configuré pour utiliser le certificat auto-émis créé par l'autorité de certification privée dans Windows EBS 2008.

Remarque

Assurez-vous que la chaîne de certificats du certificat tiers est validée par un fournisseur qui est déjà répertorié dans le magasin de certificats de l'appareil. Pour afficher la liste des fournisseurs de certificats pour les appareils Windows Mobile 6, visitez le site Web Microsoft Web site (http://www.microsoft.com/france/technet/solutionaccelerators/mobilite/deploiement-des-equipements-windows-mobile-6-avec-microsoft_exchange_server2007.mspx).

Option A : Utilisation d'un certificat auto-émis

Le serveur de messagerie et le serveur d'administration de la sécurité utilisent le certificat auto-émis par défaut généré par l'autorité de certification privée dans Windows EBS 2008.

Installation du certificat auto-émis

Le certificat auto-émis doit être installé sur l'appareil Windows Mobile.

Cette section explique comment utiliser le package d'installation de certificats fourni dans Windows EBS 2008 pour installer le certificat auto-émis sur chaque appareil mobile.

Exécutez la procédure suivante pour installer le certificat sur un appareil mobile :

1. Créez un dossier partagé dans lequel stocker le certificat auto-émis.
2. Exportez le certificat vers le dossier partagé afin que les appareils mobiles puissent y accéder.
3. Installez le certificat sur l'appareil Windows Mobile.

Pour créer un dossier partagé dans lequel stocker le fichier de certificat

1. Sur le serveur, ouvrez l'Explorateur Windows.
2. Sélectionnez le lecteur ou dossier racine dans lequel vous souhaitez créer le dossier partagé. Cliquez sur **Fichier**, pointez sur **Nouveau**, puis cliquez sur **Dossier**.
3. Assignez un nouveau nom au dossier qui soit facile à retenir (par exemple, **PartCert**).
4. Cliquez avec le bouton droit sur le dossier renommé, puis cliquez sur **Partager**.
5. Cliquez sur **Partage avancé**, puis activez la case à cocher **Partager ce dossier**.
6. Cliquez sur **Autorisations** pour ajouter les utilisateurs qui ont besoin d'accéder à ce dossier.
7. Cliquez sur **OK** pour enregistrer les modifications, puis fermez la boîte de dialogue Autorisations.

   Cliquez sur **OK** pour fermer la boîte de dialogue Partage avancé. Cliquez sur **Fermer** pour quitter la boîte de dialogue des propriétés du dossier.

Pour copier le fichier de certificat dans le dossier partagé

1. Sur le serveur d'administration, ouvrez l'Explorateur Windows.
2. Parcourez le dossier Package Cert RWW :

   %ProgramFiles%\Windows Essential Business Server\Data\Package Cert RWW
3. Copiez le fichier de certificat de sécurité (qui correspond au certificat auto-émis créé par l'autorité de certification privée dans Windows EBS 2008) dans ce dossier.
4. Collez le fichier dans le dossier partagé que vous venez de créer.

Maintenant que le certificat auto-émis a été copié dans le dossier partagé, exécutez la procédure suivante pour installer le certificat sur un appareil Windows Mobile.

Pour installer le certificat auto-émis sur un appareil Windows Mobile

1. Connectez votre appareil mobile à un ordinateur client, à l'aide de sa station d'accueil ou du câble approprié.
2. Sur l'ordinateur client, ouvrez l'Explorateur Windows, puis ouvrez le dossier partagé que vous avez créé sur le serveur, (en l'occurrence **PartCert**).
3. Copiez le fichier de certificat à partir du dossier partagé et collez-le dans le dossier système **Appareil Mobile** dans l'Explorateur Windows de l'ordinateur client. Ainsi, le certificat est placé dans le dossier **Mes documents (My Documents)** de l'appareil Windows Mobile.
4. Dans l'appareil Windows Mobile, ouvrez l'**Explorateur de fichiers**.
5. Recherchez le fichier de certificat que vous venez de copier dans le dossier **Mes documents (My Documents)** de l'appareil, puis exécutez-le soit en cliquant sur le nom de fichier, soit en le sélectionnant et en appuyant sur la touche **Entrée**.
6. Cliquez sur **Oui** dans la boîte de message de confirmation pour installer le certificat. Si aucun message d'erreur ne s'affiche, cela signifie que le certificat a été installé correctement.

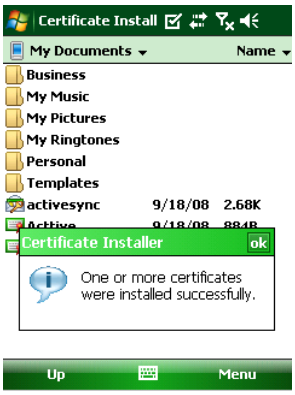

Figure 3 : Installation du certificat auto-émis sur chaque appareil Windows Mobile

Option B : Utilisation d'un certificat tiers

Avant d'installer un certificat tiers, vous devez au préalable en faire l'acquisition auprès d'une autorité de certification approuvée. Pour obtenir et installer un certificat tiers approuvé, vous devez procéder comme suit sur le serveur d'administration de la sécurité :

a. Créez une demande de signature de certificat à l'aide de l'Assistant **Créer une demande de certificat** (dans le Gestionnaire des services Internet).

b. Demandez ou achetez un certificat auprès d'un fournisseur de certificats (procédure en ligne pouvant être différente en fonction du fournisseur).

c. Enregistrez le certificat envoyé par le fournisseur de certificats sous Windows EBS 2008.

d. Installez le certificat à l'aide de l'Assistant **Terminer la demande de certificat** dans le Gestionnaire des services Internet.

e. Assignez le certificat tiers au site approprié du Gestionnaire des services Internet.

Création d'une demande de signature de certificat à l'aide de l'Assistant Créer une demande de certificat

Pour créer une demande de signature de certificat sur le serveur d'administration de la sécurité, vous devez procéder comme suit :

Connectez-vous au **Gestionnaire des services Internet** sur le serveur d'administration de la sécurité via la **Console d'administration de Windows Essential Business Server**.

1. Cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sur **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur d'administration de la sécurité dans la liste des serveurs, puis cliquez sur **Gestionnaire des services Internet** dans le volet Tâches.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur d'administration de la sécurité. Cliquez sur OK.
4. Dans le Gestionnaire des services Internet, cliquez sur le nom du serveur dans le volet **Connexions**, puis double-cliquez sur **Certificats du serveur** dans la zone **Espace de travail**.
5. Dans le volet **Actions**, cliquez sur **Créer une demande de certificat**.
6. Entrez les informations obligatoires pour le certificat à l'aide de l'Assistant **Demander un certificat**. Cliquez sur **Suivant**.

7. Conservez les paramètres par défaut définis dans **Propriétés du fournisseur de services de chiffrement**, puis cliquez sur **Suivant**.
8. Entrez un nom de fichier pour votre demande de signature de certificat.
9. Vous devez utiliser le code de signature stocké dans ce fichier lors de la demande en ligne du certificat approuvé. Lorsque vous y êtes invité, copiez le contenu du fichier dans le processus de commande en ligne.

Demande et acquisition d'un certificat auprès d'un fournisseur de certificats

Il s'agit d'un processus en ligne qui implique l'acquisition d'un certificat tiers auprès d'une autorité de certification. Ce processus peut être différent en fonction de l'autorité de certification choisie. Lors du processus d'acquisition, vous devrez fournir le contenu du fichier de demande de signature de certificat qui a été créé à l'aide de l'Assistant **Créer une demande de certificat**. Assurez-vous que les informations fournies lors de ce processus correspondent à celles fournies dans l'Assistant Demande de certificat.

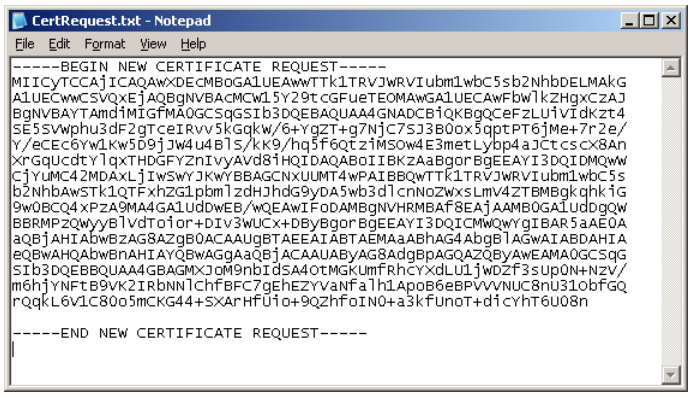

Figure 4 : Exemple du code de demande de signature de certificat généré par l'Assistant Créer une demande de certificat dans le Gestionnaire des services Internet

Remarque

Certaines autorités de certification rendent immédiatement disponible le certificat approuvé, alors que d'autres préfèrent vérifier les informations de l'utilisateur avant de lui fournir le certificat approuvé. Dans le cas de ces fournisseurs, vous pouvez réexécuter l'Assistant pour installer le certificat approuvé après l'avoir reçu.

Enregistrement d'un certificat envoyé par le fournisseur de certificats sous Windows EBS 2008

Le fournisseur de certificats peut envoyer le certificat par messagerie électronique sous la forme d'une pièce jointe compressée (fichier .zip). Extrayez le contenu et enregistrez le fichier .CER sur le serveur d'administration de la sécurité. Ce certificat doit ensuite être installé sur le Gestionnaire des services Internet.

Installation du certificat tiers fourni par l'autorité de certification

1. Cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sur **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur d'administration de la sécurité dans la liste des serveurs, puis cliquez sur **Gestionnaire des services Internet** dans le volet **Tâches**.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur d'administration de la sécurité. Cliquez sur **OK**.
4. Dans le Gestionnaire des services Internet, cliquez sur le nom du serveur dans le volet **Connexions**, puis double-cliquez sur **Certificats du serveur** dans la zone **Espace de travail**.
5. Dans le volet **Tâches**, cliquez sur **Terminer la demande de certificat**.
6. Accédez au fichier de certificat que vous avez enregistré sur le serveur d'administration de la sécurité, puis entrez un **nom convivial**. Le nom convivial attribué à un certificat permet de le distinguer facilement des autres certificats.
7. Cliquez sur OK pour installer le certificat sur le serveur.

Assignation du certificat tiers au site approprié du Gestionnaire des services Internet

Le certificat tiers approuvé doit être assigné au site Web par défaut sur le serveur de messagerie. Ce processus implique l'utilisation de l'option **Liaisons** dans le Gestionnaire des services Internet.

Pour cela, procédez comme suit :

1. Démarrez la **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur de messagerie dans la liste des serveurs, puis cliquez sur **Gestionnaire des services Internet** dans le volet Tâches.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur d'administration de la sécurité. Cliquez sur **OK**.
4. Dans le volet Connexions du **Gestionnaire des services Internet**, développez le nœud **Serveur**, développez **Sites**, puis cliquez sur **Site Web par défaut**.
5. Cliquez sur **Liaisons** dans le volet Actions.

6. Cliquez sur le bouton **Ajouter (Add)** dans la boîte de dialogue **Liaisons de sites (Site Bindings)**.
7. Cliquez sur la liste déroulante **Type**, puis sélectionnez **https**. Le Port 443 est automatiquement assigné à ce site.
8. Cliquez sur la liste déroulante **Certificat SSL (SSL certificate)**, puis sélectionnez le certificat auto-émis ou le certificat tiers approuvé que vous venez d'installer sur le serveur.
9. Cliquez sur **Afficher (View)** pour vous assurer que vous avez choisi le bon certificat. Vous pouvez également le vérifier en affichant les détails **Créé pour** et **Créé par**. Cliquez sur **OK** pour fermer la boîte de dialogue Certificat.
10. Cliquez sur **OK** pour terminer le processus.

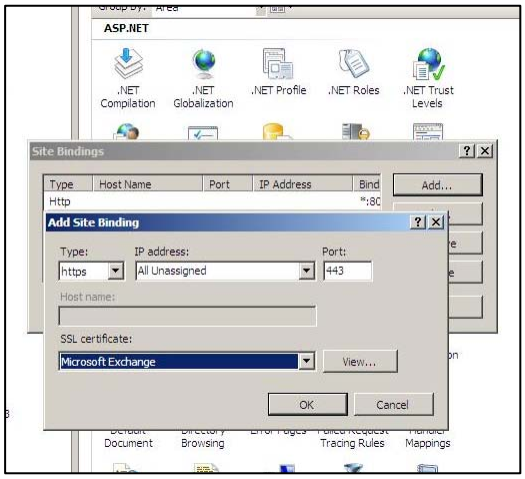

Figure 5 : Assignation du certificat tiers approuvé au port HTTPS du site Web

Remarque

Il se peut qu'une erreur de certificat se produise. Dans ce cas, cliquez sur le message d'erreur, puis sur **Afficher les certificats**. Les informations relatives au certificat s'affichent. Cliquez sur **Installer le certificat** pour que le message d'erreur ne s'affiche plus lorsque vous accédez à la page d'accueil d'Outlook Web Access (OWA).

Étape 5 : Installation et configuration du certificat tiers sur le serveur d'administration de la sécurité

Étant donné que le serveur d'administration de la sécurité fournit une protection pare-feu et antivirus Web faisant partie intégrante de la solution Windows EBS 2008, il permet donc d'isoler les réseaux externes du réseau Windows EBS 2008 interne. Pour autoriser les demandes entrantes à accéder à la boîte aux lettres Exchange sur une connexion HTTPS, vous devez procéder comme suit :

a. Installez le certificat tiers dans le magasin de certificats principaux de confiance du serveur d'administration de la sécurité.

b. Ajoutez le certificat tiers pour le port d'écoute Web externe dans Forefront TMG.

c. Enfin, installez le certificat tiers sur un appareil Windows Mobile, s'il n'est pas répertorié dans le magasin de certificats de l'appareil Windows Mobile.

Installation du certificat tiers sur le serveur d'administration de la sécurité

Pour installer le certificat tiers sur le serveur d'administration de la sécurité dans le cas d'une connexion HTTPS, vous devez procéder comme suit :

a. Exportez le certificat vers un emplacement partagé pour le serveur d'administration de la sécurité.

b. Importez le fichier de certificat dans le magasin de certificats principaux de confiance à l'aide des certificats MMC.

Ajout du certificat tiers pour le port d'écoute Web externe dans Forefront TMG

Pour configurer le Poste de travail Web à distance avec un certificat public émis par une autorité de certification approuvée, vous devez exécuter la procédure suivante. Par défaut, le port d'écoute Web externe du Poste de travail Web à distance est configuré pour utiliser le certificat qui est émis par l'autorité de certification privée dans Windows EBS. Si vous choisissez de conserver la configuration par défaut, vous devez installer un certificat principal sur les ordinateurs clients, ce qui permet de garantir un accès distant sécurisé au Poste de travail Web à distance.

Pour ajouter un certificat pour le port d'écoute Web externe, procédez comme suit :

1. Cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sur **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur l'onglet **Sécurité**, puis sur **Pare-feu réseau**, puis dans le volet Tâches, cliquez sur **Démarrer la console de Forefront Threat Management Gateway**.
3. Cliquez sur **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour afficher la console Forefront TMG sur le serveur d'administration de la sécurité.
4. Dans l'arborescence de la console Forefront TMG, développez le nom de votre serveur d'administration de la sécurité, puis cliquez sur **Stratégie de pare-feu**.
5. Dans le volet des résultats, double-cliquez sur **Règle de publication du Poste de travail Web à distance**.
6. Dans **Règle de publication du Poste de travail Web à distance**, cliquez sur l'onglet **Port d'écoute**.
7. Sélectionnez **Port d'écoute Web externe** dans la liste, puis cliquez sur **Propriétés**.
8. Dans **Propriétés du port d'écoute Web externe**, cliquez sur l'onglet **Certificats**.
9. Sélectionnez **Utiliser un certificat unique pour ce port d'écoute Web** ou **Assigner un certificat à chaque adresse IP**, puis cliquez sur **Sélectionner un certificat**.
10. Dans la boîte de dialogue **Sélectionner un certificat**, sélectionnez le certificat tiers préalablement installé, puis cliquez sur **Sélectionner**. Cliquez sur **OK** deux fois pour fermer les boîtes de dialogue **Propriétés**.
11. Pour enregistrer les modifications et actualiser la configuration, cliquez sur **Appliquer** dans le volet des résultats.

Installation du certificat tiers sur un appareil Windows Mobile

Si l'autorité de certification tierce est déjà présente dans le magasin de certificats Windows Mobile, il n'est peut être pas nécessaire de transférer et d'installer le fichier de certificat sur l'appareil. En revanche, si l'autorité de certification n'est pas répertoriée dans l'appareil Windows Mobile, vous devez exécuter la procédure suivante pour configurer et installer un certificat tiers en vue de l'utilisation sur des appareils mobiles :

1. Créez un dossier partagé dans lequel stocker le certificat.
2. Exportez le certificat vers le dossier partagé afin que les appareils mobiles puissent y accéder.
3. Installez le certificat sur l'appareil Windows Mobile.

Étape 6 : Configuration du serveur de messagerie Windows Essential Business Server 2008

Pour configurer le serveur, vous devez au préalable vous assurer que le service de site est démarré.

Vérification du démarrage du service de site

Par défaut, ce service est démarré et fonctionne sur le serveur de messagerie Windows EBS 2008. Outlook Web Access, Microsoft Exchange ActiveSync et Outlook Anywhere (anciennement connu sous le nom de RPC/HTTPS) sont également activés par défaut, et de ce fait ne requièrent pas de configuration supplémentaire.

Vous pouvez maintenant accéder à la page d'Outlook Web Access localement. Entrez https://MessagingServerName/owa.

Remarque

Il se peut qu'une erreur de certificat se produise. Dans ce cas, cliquez sur le message d'erreur, puis sur **Afficher les certificats**. Les informations relatives au certificat s'affichent. Cliquez sur **Installer le certificat** pour que le message d'erreur ne s'affiche plus lorsque vous accédez à la page d'accueil d'Outlook Web Access (OWA).

Étape 7 : Configuration de la synchronisation de l'appareil

Les appareils Windows Mobile peuvent être synchronisés avec Microsoft Exchange Server 2007 sous Windows EBS 2008, de l'une des façons suivantes :

a) Synchronisation OTA (Over-the-Air, sans fil) à partir d'un appareil Windows Mobile
b) Synchronisation réseau, via un PC client avec le Gestionnaire pour appareils Windows Mobile ou ActiveSync

Option A : Synchronisation OTA de l'appareil

Vous pouvez utiliser ActiveSync sur un appareil Windows Mobile 6 pour effectuer une synchronisation directe avec son serveur Exchange Server. L'utilisateur de l'appareil Windows Mobile doit disposer de l'adresse Exchange Server, du nom de domaine, du nom d'utilisateur et du mot de passe pour être en mesure de se connecter à la boîte aux lettres. La procédure suivante permet de configurer un appareil

Windows Mobile 6 en vue d'une connexion à la boîte aux lettres de l'utilisateur sur le serveur de messagerie.

Pour établir la connexion sans fil d'un appareil Windows Mobile 6 avec un serveur Exchange Server :

1. Dans l'écran **Accueil**, choisissez **Démarrer**, **Programmes**, puis **ActiveSync**.
2. Choisissez **Menu**, puis **Configurer le serveur**.

   Si l'appareil mobile n'a pas encore été synchronisé avec Exchange Server, l'option **Ajouter un serveur source... (Add Server Source…)** est disponible.

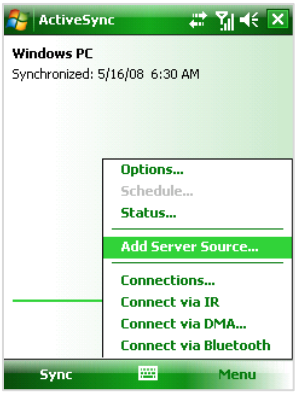

Figure 6 : Choix de l'option Ajouter un serveur source pour modifier les paramètres de serveur

3. Dans **Modifier les paramètres du serveur (Edit Server Settings)**, entrez le nom du serveur qui exécute Exchange, puis choisissez **Suivant (Next)**.

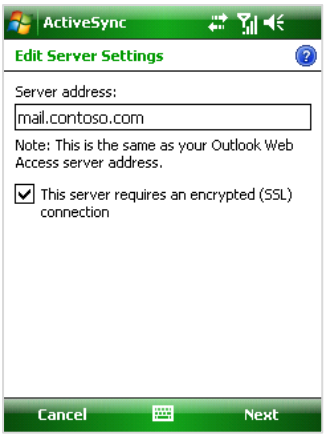

Figure 7 : Saisie du nom du serveur qui héberge la boîte aux lettres de l'utilisateur

4. Entrez le nom d'utilisateur, le mot de passe et le nom de domaine, puis choisissez **Suivant (Next)**. Activez la case à cocher **Enregistrer le mot de passe (Save password)**.

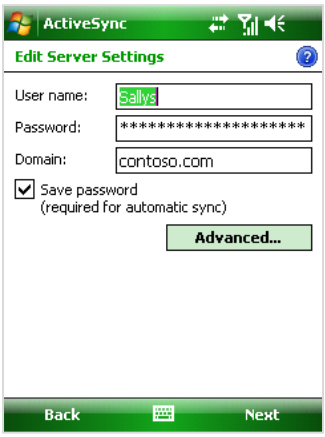

Figure 8 : Saisie du nom d'utilisateur, du mot de passe et du nom de domaine

5. Activez les cases à cocher correspondant aux informations que vous souhaitez synchroniser avec Exchange Server. Pour changer les paramètres de synchronisation disponibles, sélectionnez les informations à synchroniser, puis choisissez **Paramètres (Settings)**.

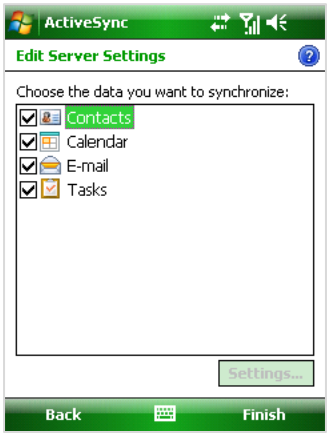

Figure 9 : Sélection des éléments à synchroniser avec Exchange Server

Choisissez **Terminer (Finish)**. L'appareil Windows Mobile tente d'accéder à la boîte aux lettres Exchange Server à partir des informations d'identification de l'utilisateur saisies préalablement. Il crée ensuite un partenariat et démarre le processus de synchronisation.

En fonction du système d'exploitation exécuté sur l'ordinateur client, la synchronisation de l'appareil utilise soit ActiveSync (pour les clients Windows XP), soit WDMC (pour les clients Windows Vista).

Option B : Synchronisation de l'appareil à l'aide d'ActiveSync

Cette section vous aide à configurer un appareil Windows Mobile en vue d'une synchronisation avec le serveur et des ordinateurs clients dotés de Microsoft ActiveSync 4.5 sous Windows XP. Pour plus de détails sur l'installation d'ActiveSync 4.5, consultez l'« Étape 1 : Installation de Microsoft ActiveSync 4.5 », figurant plus haut dans ce document.

Pour configurer un appareil Windows Mobile en vue d'une synchronisation avec Windows EBS

1. Connectez l'appareil Windows Mobile à un ordinateur client. La méthode de connexion dépend des capacités de l'appareil et de l'ordinateur. La connexion est généralement de type USB, série, Bluetooth ou à port infrarouge.

   Remarque

   ActiveSync 4.5 doit être installé sur l'ordinateur client Windows XP.

2. Après avoir connecté l'appareil à un ordinateur client, l'Assistant Installation de la synchronisation s'ouvre automatiquement sur l'ordinateur client.

   Remarque

   Si l'appareil a déjà été configuré une première fois, les écrans sont différents de ceux présentés ici.

3. Cliquez sur **Suivant** sur la page **Accueil**.
4. Sur la page **Synchroniser directement avec un serveur (Synchronize directly with a server)**, activez la case à cocher **Synchroniser directement avec un serveur exécutant Microsoft Exchange Server (Synchronize directly with a server running Microsoft Exchange Server)**, puis cliquez sur **Suivant (Next)**.

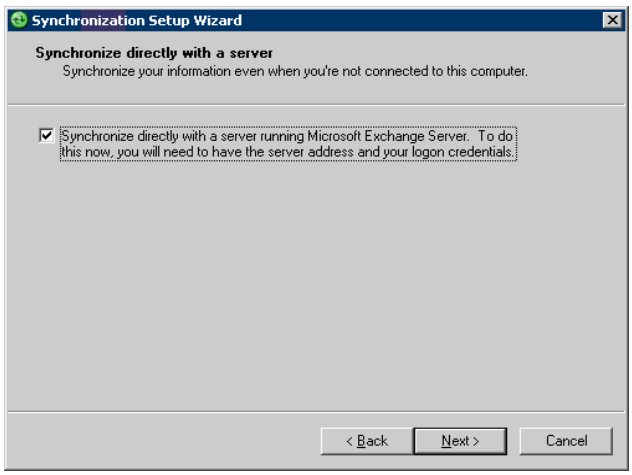

Figure 10 : Configuration de l'appareil Windows Mobile pour une synchronisation avec un serveur Microsoft Exchange Server sans connexion à un ordinateur

5. Sur la page **Informations d'identification pour le serveur Exchange (Exchange server credentials)**, indiquez le nom DNS public du serveur ainsi que les références d'identification de l'utilisateur. Activez les cases à cocher **Ce serveur exige une connexion cryptée (This server requires an encrypted (SSL) connection)** et **Enregistrer le mot de passe (Save password)**. Cliquez sur **Suivant (Next)**.

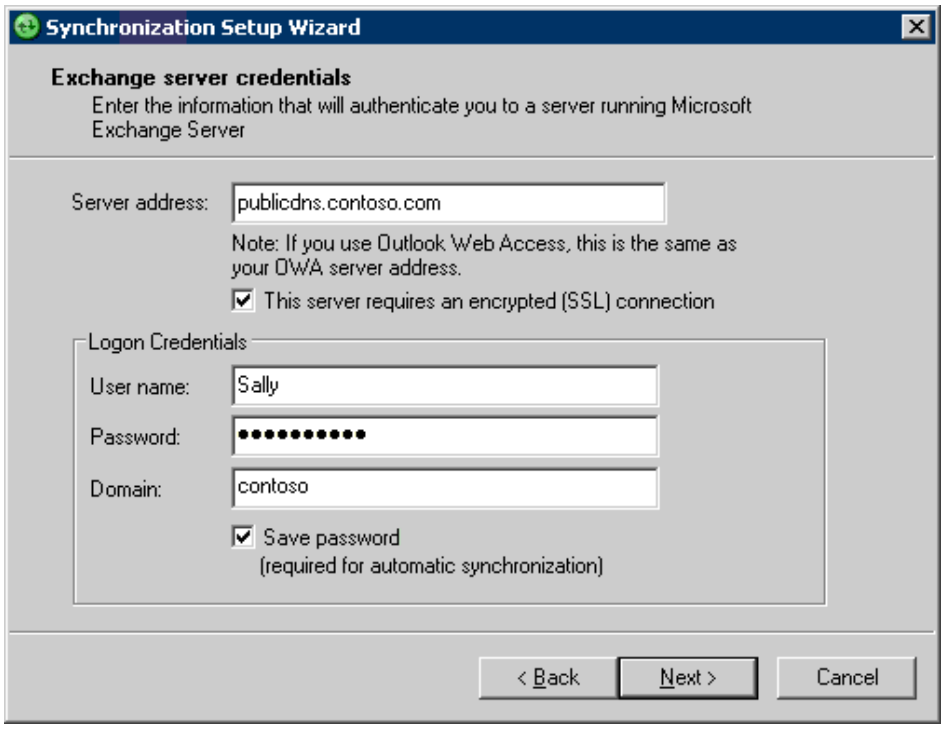

Figure 11 : Saisie d'informations d'identification permettant d'authentifier l'utilisateur sur un serveur Microsoft Exchange Server

ActiveSync tente de se connecter au serveur.

Figure 12 : ActiveSync tente de se connecter au serveur

Si des erreurs se produisent lors de la tentative, consultez la section « Résolution des problèmes » plus loin dans ce document.

6. Sur la page **Options de synchronisation (Synchronization Options)**, sélectionnez les éléments que l'appareil doit synchroniser. Sélectionnez **Exchange Server** en tant que **Source** pour Contacts, Calendrier (Calendar), Tâches (Tasks) et Courrier (E-mail). Les autres éléments tels que Multimédia (Media) et Favoris (Favorites) ne peuvent être synchronisés qu'avec l'ordinateur client.

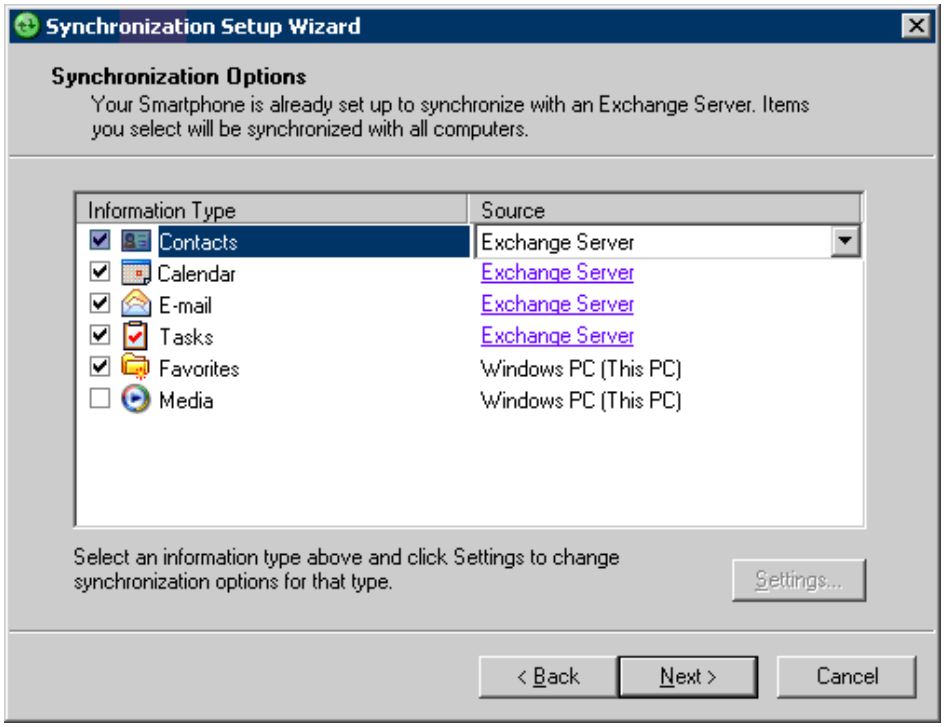

Figure 13 : Sélection du serveur Exchange Server comme Source pour les éléments à synchroniser sur le serveur

7. Cliquez sur **Suivant (Next)**, puis sur **Terminer (Finish)** pour mettre fin à l'exécution de l'Assistant.

Synchronisation de l'appareil à l'aide du Gestionnaire pour appareils Windows Mobile (WMDC)

Cette section vous aide à configurer un appareil Windows Mobile en vue d'une synchronisation avec le serveur et des ordinateurs clients dotés du Gestionnaire pour appareils Windows Mobile installé sous Windows Vista. Pour plus de détails sur l'installation du Gestionnaire pour appareils Windows Mobile (WMDC), consultez l'« Étape 1 : Installation de Microsoft ActiveSync 4.5 ou WMDC », figurant plus haut dans ce document.

Pour configurer un appareil Windows Mobile en vue d'une synchronisation avec Windows EBS

1. Connectez l'appareil Windows Mobile à l'ordinateur client. La méthode de connexion dépend des capacités de l'appareil et de l'ordinateur. La connexion est généralement de type USB, série, Bluetooth ou à port infrarouge.

Remarque

Le Gestionnaire pour appareils Windows Mobile (WMDC) doit être installé sur l'ordinateur client Windows Vista.

2. Après avoir connecté l'appareil à l'ordinateur client, cliquez sur **Démarrer**, **Programmes** puis sur **Gestionnaire pour appareils Windows Mobile**.

Remarque

Si l'appareil a déjà été configuré une première fois, les écrans suivants sont différents de ceux présentés ici.

3. Cliquez sur **Configurer votre appareil (Set up your device**) sur la page d'accueil.

Figure 14 : Utilisation du Gestionnaire pour appareils Windows Mobile pour configurer votre appareil

4. La page suivante vous invite à cocher les éléments à synchroniser. Sur cette page, vous pouvez voir les éléments Contacts, Calendrier (Calendar), Courrier (E-mail), Tâches (Tasks), etc. Cliquez sur **Suivant (Next)** pour continuer.

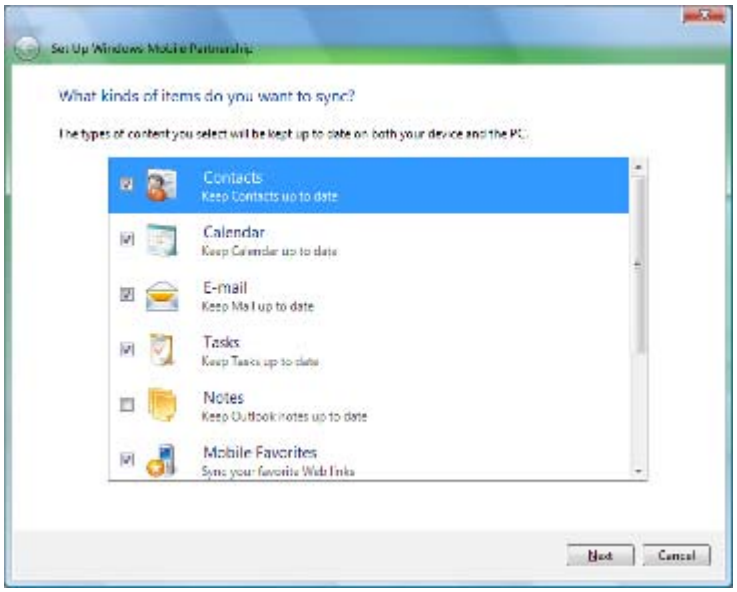

Figure 15 : Sélection des éléments à synchroniser avec le serveur Microsoft Exchange Server

5. Cette page vous invite à entrer des informations spécifiques sur votre serveur Exchange Server. Sur cette page, vous pouvez saisir l'**Adresse du serveur (Server address)**, le **Nom d'utilisateur (User name)**, le **Mot de passe (Password)** et le **Domaine (Domain)** de votre serveur Exchange Server.
   Si le serveur exige une connexion cryptée (SSL), il faut alors cocher la case correspondante. Si vous le souhaitez, vous pouvez choisir de mémoriser votre mot de passe. Cliquez sur **Suivant (Next)** pour continuer. Le Gestionnaire pour appareils Windows Mobile tente de se connecter au serveur.

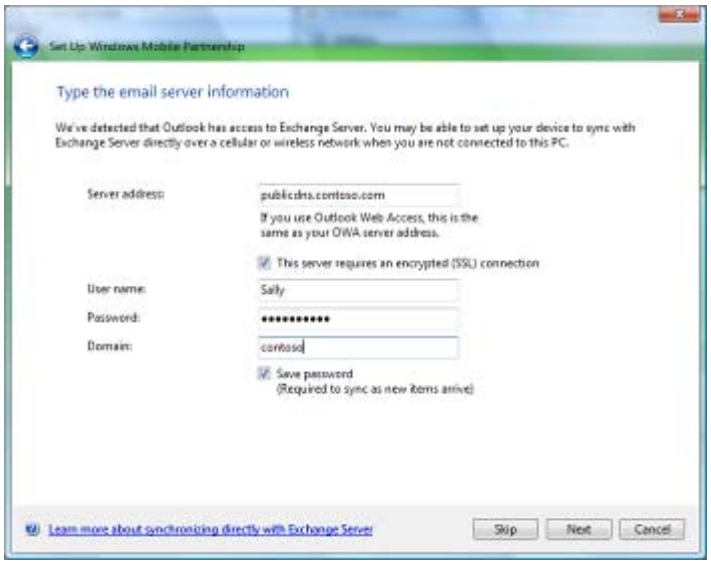

Figure 16 : Saisie d'informations d'identification sur le serveur de messagerie permettant d'authentifier l'utilisateur sur un serveur Microsoft Exchange Server

6. Une barre de progression indique le niveau d'avancement du Gestionnaire pour appareils Windows Mobile dans sa tentative de créer un partenariat entre votre appareil Windows Mobile et le serveur Exchange Server.

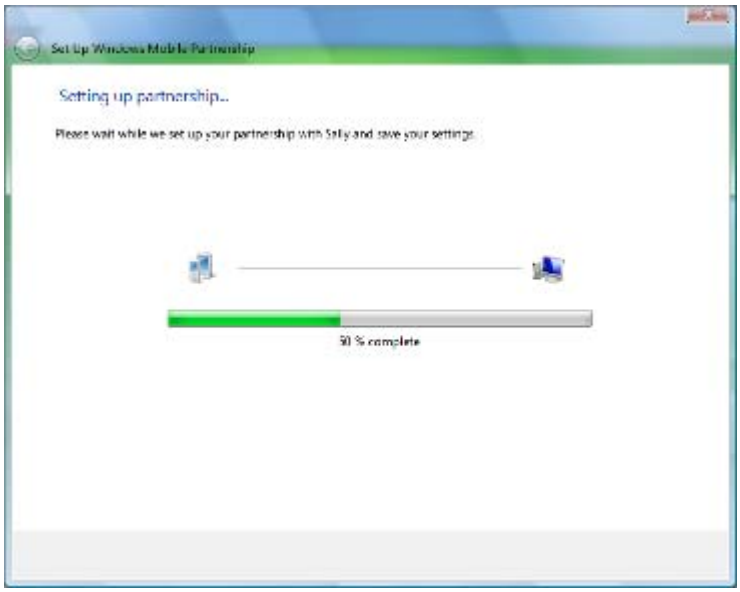

Figure 17 : Le Gestionnaire pour appareils Windows Mobile utilise les informations d'identification pour créer le partenariat avec le serveur de messagerie

7. À la fin de la synchronisation, l'application revient à la page d'accueil à partir de laquelle vous pouvez accéder aux programmes et services (Programs and Services), aux fichiers multimédias (Pictures, Music and Video), à la gestion de fichiers (File Management) et aux paramètres de l'appareil mobile (Mobile Device Settings).

Figure 18 : Utilisation de l'écran Accueil pour accéder aux services et aux paramètres de l'appareil

8. À présent, cliquez sur Paramètres de l'appareil mobile (Mobile Device Settings) pour développer la liste des options complémentaires. Cliquez sur **Autres options>> (More>>)** pour continuer.

Figure 19 : Paramètres de l'appareil mobile permettant de configurer les paramètres de synchronisation

9. Cliquez sur **Modifier les paramètres de synchronisation de contenu (Change content sync settings)**.

Figure 20 : Configuration des paramètres de synchronisation de contenu dans le Gestionnaire pour appareils Windows Mobile

10. L'écran à partir duquel vous pouvez sélectionner les paramètres de synchronisation du contenu du téléphone Windows Mobile s'affiche.

Figure 21 : Configuration des paramètres de synchronisation de chaque élément via le Gestionnaire pour appareils Windows Mobile

Étape 8 : Test du déploiement

Cette section permet de vous guider dans le test du déploiement des appareils mobiles.

Test de la synchronisation OTA

Pour tester la configuration de la synchronisation OTA ActiveSync sur l'appareil

1. Assurez-vous que l'appareil n'est pas connecté à l'ordinateur client, ni à un réseau local sans fil avec accès Internet.
2. Assurez-vous que la connectivité des données sans fil à Internet (GPRS, par exemple) est disponible sur l'appareil.
3. Ouvrez ActiveSync sur l'appareil et commencez la synchronisation.

   L'appareil se connecte à Internet, s'il n'est pas déjà connecté, et synchronise les éléments que vous avez sélectionnés lors de la configuration d'ActiveSync.

   Si la synchronisation ne fonctionne pas pour quelque raison que ce soit, reportez-vous à la section « Résolution des problèmes » plus loin dans ce document.

Test de la technologie Direct Push

Pour tester la configuration de la technologie Direct Push

1. Assurez-vous que l'appareil mobile n'est pas connecté à un ordinateur client, ni à un réseau local sans fil avec accès Internet.
2. Assurez-vous que la connectivité des données sans fil à Internet (GPRS, par exemple) est disponible sur l'appareil.
3. Envoyez un message au compte d'utilisateur pour lequel l'appareil est configuré.
4. Vérifiez que l'appareil reçoit le nouveau message immédiatement.

Remarque

La technologie Direct Push n'est pas utilisée pour la synchronisation lorsque l'appareil est connecté à un ordinateur ou à un réseau local sans fil avec accès Internet.

Gestion à distance

Windows Mobile 6 offre plusieurs nouvelles fonctionnalités qui vous permettent de mieux gérer les appareils mobiles et de mieux en protéger les données. Cette section permet de vous guider dans l'utilisation des deux fonctionnalités suivantes :

- Effacement à distance des données de l'appareil
- Règles de sécurité de l'appareil

Effacement à distance des données de l'appareil

La fonctionnalité d'effacement à distance des données de l'appareil vous permet d'effacer toutes les informations contenues sur un appareil en étant à distance. Ainsi, si un utilisateur égare un appareil, les données de la société ne sont pas compromises. La fonctionnalité Effacement à distance des données de l'appareil est activée depuis la console de gestion Exchange sur le serveur de messagerie.

Remarque

La fonctionnalité d'effacement à distance des données de l'appareil permet également de supprimer les données de n'importe quelle carte de stockage insérée dans l'appareil. Avant de tester cette fonctionnalité, assurez-vous que les données importantes contenues dans l'appareil Windows Mobile ont été correctement sauvegardées. Si vous envisagez de conserver des données sur la carte de stockage, retirez-la avant d'activer l'effacement à distance des données de l'appareil.

Pour effacer à distance toutes les informations de l'appareil

1. Démarrez la console d'administration sur le Serveur d'administration. Pour cela, cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sélectionnez **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur de messagerie dans la liste des serveurs, puis cliquez sur **Console de gestion Exchange** dans le volet Tâches du serveur de messagerie.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de messagerie. Cliquez sur **OK**.
4. Développez **Configuration du destinataire** dans l'arborescence de la console, puis sélectionnez **Boîte aux lettres**.
5. Sélectionnez l'utilisateur dans le volet Boîte aux lettres.
6. Dans le volet Action, cliquez sur **Gérer le périphérique mobile** (**Manage Mobile Device)** ou cliquez avec le bouton droit sur la boîte aux lettres de l'utilisateur, puis cliquez sur **Gérer le périphérique mobile (Manage Mobile Device)**.

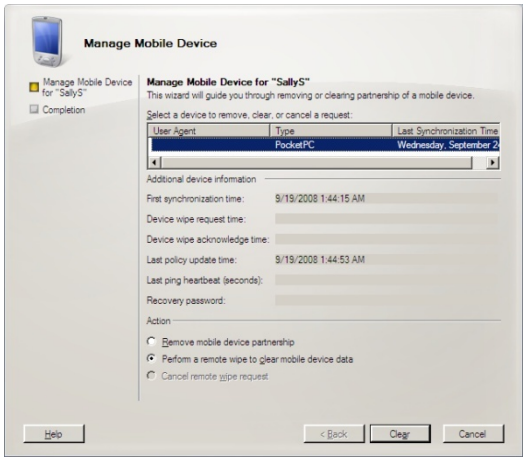

Figure 22 : Effacement à distance des données d'un appareil Windows Mobile depuis la console de gestion Exchange

7. Sélectionnez l'appareil mobile sur lequel effacer les données.
8. Dans la section Action, cliquez sur la case d'option **Effectuer un effacement à distance pour supprimer les données d'un appareil mobile (Perform a remote wipe to clear mobile device data)**.
9. Cliquez sur **Effacer (Clear)** en bas de la fenêtre pour terminer.

Règles de sécurité de l'appareil

Vous pouvez appliquer des règles de sécurité sur les appareils Windows Mobile 6, comme la configuration d'un mot de passe ou de certaines fonctionnalités d'appareils. Cela permet de protéger les informations qui sont stockées sur les appareils mobiles. Vous pouvez configurer des règles de sécurité d'appareil avec Exchange Server 2007 sur le serveur de messagerie.

Pour définir et appliquer des règles de sécurité pour les appareils mobiles

1. Sur le serveur d'administration, démarrez la console d'administration. Pour cela, cliquez sur **Démarrer**, **Tous les programmes**, **Windows Essential Business Server**, puis sélectionnez **Console d'administration de Windows Essential Business Server**.
2. Cliquez sur **Ordinateurs et périphériques**. Sélectionnez le serveur de messagerie dans la liste des serveurs, puis cliquez sur **Console de gestion Exchange** dans le volet Tâches du serveur de messagerie.
3. Cliquez sur le bouton **Connexion**, puis entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de messagerie. Cliquez sur **OK**.
4. Développez **Configuration de l'organisation**, puis **Accès client**.
5. Cliquez avec le bouton droit sur **Stratégie de boîte aux lettres ActiveSync Exchange**, puis cliquez sur **Propriétés** dans le volet Actions.

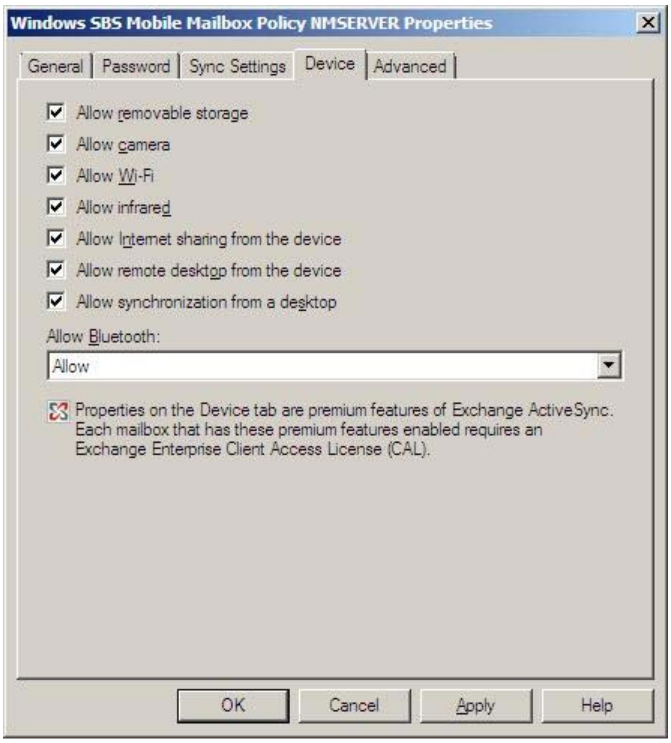

Figure 23 : Configuration de l'accès à l'appareil de l'utilisateur en modifiant la stratégie de boîte aux lettres

Pour créer une nouvelle règle de boîte aux lettres

1. Cliquez sur **Nouvelle stratégie de boîte aux lettres ActiveSync Exchange** dans le volet Actions.

   La nouvelle stratégie peut être assignée à chaque appareil à partir des propriétés utilisateur.
2. Développez **Configuration du destinataire**, puis sélectionnez **Boîte aux lettres**.
3. Double-cliquez sur l'utilisateur pour afficher ses propriétés. Cliquez sur l'onglet **Fonctionnalités de boîte aux lettres**.
4. Sélectionnez **Exchange ActiveSync**, puis cliquez sur le bouton **Propriétés**.
5. Cliquez sur **Parcourir** pour changer la stratégie de boîte aux lettres ActiveSync Exchange assignée à l'appareil.

Pour afficher la liste des paramètres de stratégie ActiveSync par défaut, visitez le site suivant :

Microsoft Web site (http://technet.microsoft.com/fr-fr/library/bb123484.aspx)

Conclusion

Windows Essential Business Server 2008 vous permet de déployer une solution de messagerie Windows Mobile au sein de votre organisation d'une manière simple et sécurisée. Le Serveur d'administration de la sécurité fournit une couche de protection supplémentaire contre les intrusions et les infections virales. Sa solution totalement intégrée et l'expérience de l'administration simplifient le déploiement des appareils Windows Mobile au sein d'un réseau. Grâce à la nouvelle version de la Console d'administration de Windows Essential Business Server sur le serveur d'administration, vous pouvez contrôler à distance la sécurité et les serveurs de messagerie avec efficacité. En d'autres termes, ce document a été conçu pour vous aider à déployer les appareils Windows Mobile sur un réseau Windows EBS 2008 sans presqu'aucun effort.

Résolution des problèmes

Cette section fournit des conseils et des procédures de résolution des problèmes pouvant se produire lors du déploiement des appareils Windows Mobile. Ces conseils et procédures sont répertoriés dans les sections suivantes :

- Installation d'ActiveSync sur les ordinateurs clients
- Configuration d'ActiveSync
- Synchronisation de l'appareil mobile
- Accès à l'outil d'administration Web ActiveSync Exchange Server
- Déploiement des certificats
- Configuration de l'appareil

Installation de Microsoft ActiveSync sur les ordinateurs clients

Si Microsoft ActiveSync 4.5 n'est pas installé correctement sur un ordinateur client, procédez comme suit :

- Assurez-vous que vous êtes bien connecté en tant qu'administrateur local sur l'ordinateur. Le logiciel ne peut être installé sans droits d'administration locaux.
- Si vous utilisez la Stratégie de groupe pour installer ActiveSync, vérifiez les points suivants :
    - Les listes de contrôle d'accès doivent être définies correctement sur l'objet de stratégie de groupe (GPO).

- Le groupe Utilisateurs authentifiés ne doit pas figurer dans la liste et les options d'autorisations de lecture et d'application de la stratégie de groupe doivent être activées pour le groupe Utilisateurs mobiles Windows EBS.
- L'objet de stratégie de groupe doit être lié à l'unité organisationnelle correspondante. Si un compte utilisateur est configuré en tant que composant de l'unité organisationnelle SBSUsers, il est associé à l'objet de stratégie de groupe par défaut. Dans ce cas, ActiveSync 4.5 est déployé automatiquement sur les ordinateurs clients qui sont définis dans la stratégie de groupe. Si vous n'avez pas utilisé les Assistants de configuration des nouveaux utilisateurs pour créer des comptes d'utilisateur ou si les comptes d'utilisateur ne figurent pas dans l'unité organisationnelle SBSUsers pour quelque raison que ce soit, ActiveSync ne sera pas installé lorsque les utilisateurs se connecteront.

Configuration d'ActiveSync

Voici quelques erreurs pouvant se produire lors de la configuration d'ActiveSync :

- L'erreur suivante indique un problème lié à la connectivité SSL avec le serveur.

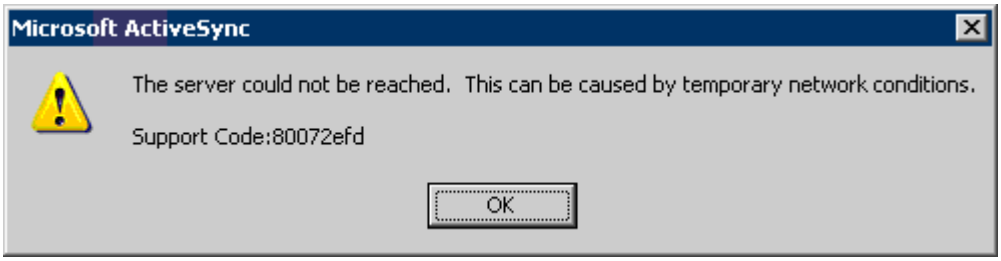

Figure 24 : Les problèmes de connectivité SSL peuvent générer ce type d'erreur

Pour résoudre ce problème, consultez la section « Recherche des problèmes liés aux certificats » plus loin dans ce document.

- Lors de la configuration du serveur, l'erreur suivante indique que l'appareil ne peut pas atteindre le serveur. Lorsque cette erreur se produit, l'appareil n'a pas atteint le seuil de vérification du certificat.

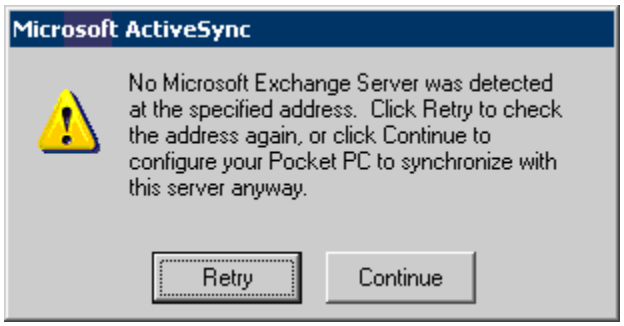

Figure 25 : L'erreur suivante indique que l'appareil est incapable d'atteindre le serveur

Vérifiez la configuration du pare-feu ainsi que la connectivité IP.

- Lors de la configuration du serveur, l'erreur suivante indique que l'appareil peut atteindre le serveur, mais que le certificat présente un problème.

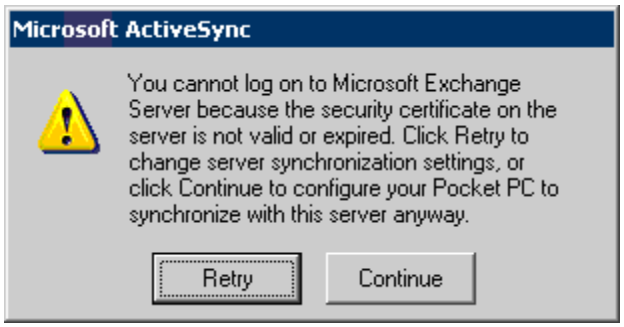

Figure 26 : L'erreur suivante indique un problème lié au certificat de sécurité

En fonction du type de certificat que vous utilisez, exécutez l'une des opérations suivantes :

- Si vous utilisez un certificat tiers, il y a un problème avec le certificat de serveur. Essayez d'accéder au serveur à partir d'un ordinateur connecté à Internet en recourant à la procédure de la section « Recherche des problèmes liés aux certificats » plus loin dans ce document.
- Si vous êtes redirigé vers une connexion SSL sans demande de certificat, vérifiez que le certificat est bien émis par une autorité de certification répertoriée dans la liste de prise en charge Windows Mobile. Les appareils Windows Mobile ne sont pas en mesure de prendre en charge autant d'autorités de certification principales que les ordinateurs de bureau dotés de Windows. Votre autorité de certification peut être approuvée sur les ordinateurs de bureau Windows mais pas sur les appareils Windows Mobile.
- Si vous n'êtes pas redirigé vers une connexion SSL et qu'un certificat vous est demandé, vérifiez que vous disposez du certificat adéquat (certificat de serveur Web). Vous pouvez également tenter de réinstaller le certificat sur le serveur en suivant les instructions fournies à la section « Option B : Utilisation d'un certificat tiers » figurant au début du document. Si aucune de ces procédures ne fonctionnent, prenez contact avec l'autorité de certification pour résoudre le problème.

- Si vous utilisez un certificat auto-émis, il se peut que le certificat ne soit pas installé sur l'appareil. Cliquez sur **Continuer**, puis installez le certificat une fois que l'Assistant a terminé. Vous ne pouvez pas effectuer de synchronisation tant que le certificat n'est pas installé sur l'appareil.

- Si vous avez déjà installé le certificat sur l'appareil, il y a un problème avec le certificat. Consultez la section « Recherche des problèmes liés aux certificats » plus loin dans ce document pour procéder aux vérifications suivantes :
  - Assurez-vous que le certificat est installé correctement sur le serveur.
  - Assurez-vous que le certificat est installé correctement sur l'appareil.

  Essayez de réinstaller le certificat sur l'appareil. Vérifiez que vous avez bien reçu un message sur l'appareil disant que le certificat a été ajouté avec succès au magasin principal.

Synchronisation de l'appareil mobile

Certains utilisateurs ne peuvent pas synchroniser

Si certains utilisateurs ne peuvent pas synchroniser leurs appareils, alors que d'autres y parviennent, effectuez les vérifications suivantes :

- Dans Exchange Management Console, dans l'onglet **Fonctionnalités de boîte aux lettres** de la boîte de dialogue des propriétés du compte d'utilisateur, assurez-vous que tous les services sont définis sur Activé.
- Vérifiez que l'appareil dispose d'un accès Internet en essayant de consulter un site à partir de l'appareil.
- Certains opérateurs nécessitent une mise à jour SIM pour utiliser le service d'accès aux données. Vérifiez auprès de votre opérateur de téléphonie mobile que vous disposez de la configuration nécessaire.
- Assurez-vous que l'heure et le fuseau horaire sont correctement définis sur l'appareil.
- Certains appareils mettent l'adresse IP des noms de domaines DNS dans le cache. Si votre serveur utilise une adresse IP dynamique avec des services Internet tels que DynDNS.org, vous devez probablement réinitialiser l'appareil en cas de modification de l'adresse IP.

Aucun utilisateur ne peut synchroniser

Si aucun utilisateur ne parvient à synchroniser son appareil, effectuez les vérifications suivantes :

- Recherchez les problèmes liés aux certificats.
- Vérifiez le journal d'événements d'applications.
- Vérifiez la configuration du pare-feu.

Recherche des problèmes liés aux certificats

Pour rechercher les problèmes liés aux certificats, procédez comme suit :

- Si vous utilisez un certificat tiers, vérifiez le certificat sur le serveur. Pour cela, accédez à l'adresse http://VotreDNSPublic.VotreServeur.com/exchange sur un ordinateur disposant d'un accès Internet (non connecté à votre réseau local), puis vérifiez que vous êtes redirigé vers une connexion SSL sans demande de certificat.
- Lorsque vous synchronisez un appareil, cliquez sur **Attention requise** sur l'écran ActiveSync. Lisez le message d'erreur pour voir s'il fait référence à un problème de certificat.
- Si vous utilisez un certificat auto-émis, assurez-vous qu'il est correctement installé sur l'appareil. Pour cela, accédez à l'adresse http://VotreDNSPublic.VotreServeur.com/exchange à partir de l'appareil, puis vérifiez que vous êtes redirigé vers une connexion SSL sans demande de certificat.
- Vous recevrez peut-être un message d'erreur si vous essayez d'installer un certificat auto-signé sur l'appareil en suivant les instructions fournies dans ce document. Dans ce cas, essayez d'exporter manuellement le certificat à partir d'un ordinateur client connecté au serveur, au lieu d'utiliser les fichiers du répertoire \\server\clientapps\ebscert. Vous pouvez exporter le certificat à partir du dossier Autorités de certification principale de confiance\Certificats dans la console Certificats et l'ouvrir en exécutant certmgr.msc lorsque vous y êtes invité.

Remarque

L'outil certinst.exe est installé sur de nombreux appareils par les fabricants. Il vous permet d'ajouter un certificat en l'ouvrant sur l'appareil, comme indiqué dans ce document.

Vérification du journal d'événements d'applications

Consultez le journal d'événements d'applications pour voir s'il contient des erreurs liées à ActiveSync.

Vérification de la configuration du pare-feu

Pour vérifier la configuration du pare-feu, procédez comme suit :

- Assurez-vous que le port 443 est ouvert et que le trafic en direction de ce port est redirigé vers le serveur.
- Assurez-vous que les recherches de chaînes d'agent utilisateur sont désactivées. Cette option est activée par défaut sur certains pare-feux. Exchange ActiveSync n'envoie pas de chaînes d'agent utilisateur.
- Assurez-vous que la valeur du délai d'attente est suffisamment élevée pour les connexions SSL. Cette valeur est généralement fixée à 15 minutes.
- Pour plus d'informations, consultez l'article 905013, « Configuration du pare-feu de l'entreprise pour la technologie ActiveSync Direct Push Exchange » à l'adresse suivante : Microsoft Web site (http://support.microsoft.com/kb/905013).

Si vous utilisez ISA Server, vous devrez peut-être implémenter une configuration DNS partagée pour assurer une certaine cohérence à l'intérieur et à l'extérieur du réseau local. Pour plus d'informations, consultez l'article « You Need to Create a Split DNS! » (Vous devez créer un DNS partagé) à l'adresse suivante : ISAServer.org Web site (http://go.microsoft.com/fwlink/?LinkID=75118).

Déploiement des certificats

Obtention d'un certificat

Si vous rencontrez des difficultés pour obtenir un certificat tiers, effectuez les vérifications suivantes :

- Assurez-vous que les informations de Dun & Bradstreet (D&B) ou d'un autre annuaire commercial concernant votre entreprise sont à jour avant de demander un certificat. Vous pouvez vérifier les informations D&B à l'adresse suivante : Microsoft Web site (http://dbfrance.dnb.com/French/default.html).
- Si vous disposez d'un nom de marque, assurez-vous qu'il est inclus dans vos informations D&B. Préparez-vous à fournir des preuves de ce nom de marque. Des exemples d'éléments communément acceptés par les autorités de certification principales pour émettre un certificat incluent les statuts constitutifs, la licence commerciale et les informations D&B.
- En fonction de la demande de certificat émise, préparez-vous comme suit :
  - Si vous utilisez un nom de marque ou une raison sociale : fournissez une licence d'exploitation, une photocopie de votre facture d'électricité, un relevé bancaire ou un autre justificatif contenant le nom de marque et le nom de la société.
  - Si vous utilisez un nom personnel : fournissez une photocopie de votre permis de conduire ou de votre passeport. Les conditions requises varient selon les autorités de certification, mais toutes vérifieront votre identité avant d'émettre un certificat. Les informations fournies à l'autorité de certification doivent correspondre exactement aux informations entrées dans la demande de signature du certificat d'origine. Par exemple, si les statuts constitutifs indiquent une adresse différente de l'adresse fournie dans la demande de signature du certificat, le certificat ne sera pas émis.

Création d'une demande de signature de certificat

Effectuez les vérifications suivantes lors de la création d'une demande de signature de certificat :

- Assurez-vous qu'il n'existe aucun certificat sur le serveur. Si un certificat existe, vous devez le supprimer avant de créer la nouvelle demande de signature de certificat.
- Si vous avez installé un certificat provenant d'une autorité de certification sur le serveur, assurez-vous que la demande de certificat n'est pas envoyée automatiquement à une autorité en ligne. Sinon, vous ne créerez pas un certificat tiers.

Installation d'un certificat auto-émis

Voici quelques problèmes qui peuvent se produire lors de l'installation d'un certificat auto-émis sur un appareil mobile :

- L'exécution du certificat après l'avoir copié sur l'appareil n'installe pas correctement le certificat (ajout au magasin principal).

  Vous devrez peut-être utiliser *certinstaller.exe* pour installer le certificat dans le magasin principal. Pour obtenir des instructions, consultez la section « Option A : Utilisation d'un certificat auto-émis » au début du document.

Configuration de l'appareil

Messages Direct Push

Assurez-vous que l'appareil n'est pas connecté à un ordinateur, ni à un réseau local sans fil.

La technologie Direct Push fonctionne uniquement avec la synchronisation OTA.

Stratégie de l'appareil

Si les nouvelles stratégies exécutées sur l'appareil ne sont pas appliquées, assurez-vous que l'appareil a été synchronisé après la mise à jour de la stratégie. Les stratégies sont appliquées pendant le cycle ActiveSync et les nouvelles stratégies ne sont pas appliquées avant la synchronisation suivante.

Lorsque la stratégie est appliquée à un appareil, l'utilisateur est invité à mettre son appareil en conformité avec la nouvelle stratégie, en définissant un mot de passe par exemple.

Synchronisation

Si une synchronisation lancée par un utilisateur échoue sur l'appareil :

- Vérifiez que vous avez accès à Outlook Web Access (OWA). Vous vous assurez ainsi de la connectivité du serveur et de l'absence d'erreurs liées au certificat.
- Vérifiez la connectivité Internet sans fil depuis l'appareil. Si l'appareil n'a pas de connectivité Internet sans fil, contactez l'opérateur de téléphonie mobile.
- Vérifiez les journaux IIS sur le serveur. Recherchez les entrées provenant de l'appareil mobile et vérifiez l'existence de messages d'erreur qui pourraient permettre d'identifier le problème.
- Activez la connexion sur l'appareil et consultez les journaux pour rechercher les entrées susceptibles de donner plus d'informations sur le problème. Pour activer la connexion sur l'appareil, suivez les étapes ci-dessous :
  - **Si vous avez un appareil Windows Mobile Standard :**

    a. Cliquez sur **Démarrer**, **Programmes**, puis sélectionnez **ActiveSync**.

    b. Cliquez sur **Menu**, puis sélectionnez **Configurer le serveur**.

    c. Cliquez sur **Suivant**, puis sur **Avancé**.
  - **Si vous avez un appareil Windows Mobile Classic ou Professional :**

    a. Cliquez sur **Démarrer**, puis sélectionnez **ActiveSync**.

    b. Cliquez sur **Menu**, **Configurer le serveur**, **Suivant**. Cliquez une nouvelle fois sur **Suivant**, puis sur **Menu** et **Avancé**.

    c. Modifiez le niveau de journalisation et sélectionnez **Commentaires**. Les journaux sont stockés sur l'appareil dans le dossier **Windows\ActiveSync**.

    d. Cliquez sur **Suivant**, puis sur **Terminer**.

Liens connexes

Pour plus d'informations sur Windows EBS, reportez-vous à « Windows Essential Business Server 2008 » à l'adresse suivante : Microsoft Web site (www.ebs-2008.fr).