Microsoft Windows Server System

Guide d'accès client pour Exchange Server 2003

Dernière mise à jour :	août 2004
Version du produit :	Exchange Server 2003
Révisé par :	Équipe de développement Exchange
Informations récentes :	www.microsoft.com/exchange/library
Auteur :	Joey Masterson

Guide d'accès client pour Exchange Server 2003

Joey Masterson

Date de publication : avril 2004
Mise à jour : août 2004
S'applique à : Exchange Server 2003

Copyright

Remerciements

Éditeur du projet : Diane Forsyth

Réviseurs techniques : Équipe produit Exchange

Conception graphique : Kristie Smith

Production : Joe Orzech, Sean Pohtilla

Table des matières

Introduction

Ce guide fournit des informations essentielles sur l'utilisation de Microsoft® Exchange Server 2003 et l'accès client. Il présente les nouvelles fonctionnalités de Microsoft Exchange 2003 et Microsoft Office Outlook® 2003, en plus des améliorations apportées à Microsoft Office Outlook Web Access 2003. Il contient des informations sur les tâches de configuration, comme la sécurisation de l'environnement de messagerie, le déploiement de l'architecture serveur et la configuration de serveurs Exchange pour les méthodes d'accès client prises en charge. Enfin, ce guide traite de la façon de gérer les protocoles, le serveur virtuel Exchange, Outlook Web Access, ActiveSync® Exchange et Microsoft Outlook Mobile Access.

À qui s'adresse ce guide ?

Toute personne ayant une formation technique peut tirer parti de la lecture de ce guide, mais ce dernier est principalement destinés aux professionnels suivants :

Architectes système
Personnes responsables de la planification et de l'élaboration des stratégies et des solutions de l'entreprise.

Administrateurs Exchange de l'entreprise
Personnes responsables de l'installation, de la maintenance et de l'administration des logiciels dans l'entreprise.

Gestionnaires de comptes d'utilisateur Exchange
Personnes responsables de la configuration des comptes individuels de messagerie et de la modification des comptes individuels Exchange dans le service d'annuaire Microsoft Active Directory®.

Responsables d'assistance Messagerie
Personnes spécialisées dans la résolution des problèmes rencontrés par les utilisateurs finaux avec leur environnement de messagerie.

Opérateurs de support technique
Personnes chargées d'apporter une assistance aux utilisateurs finaux dans divers domaines logiciels et matériels, notamment les problèmes de messagerie simples.

Comment ce guide est-il structuré ?

Ce guide comporte trois chapitres et une annexe. Pour obtenir des résultats optimaux, passez ces chapitres en revue dans l'ordre prévu, car chacun d'eux s'appuie sur des concepts étudiés dans les chapitres précédents.

Chapitre 1, « Présentation de Microsoft Exchange Server 2003 et de l'accès client »
Ce chapitre donne une vue d'ensemble des nouvelles fonctionnalités de Microsoft Exchange 2003 et Outlook 2003.

Chapitre 2, « Configuration de Microsoft Exchange Server 2003 pour l'accès client »
Ce chapitre fournit des informations sur la configuration de Microsoft Exchange 2003 pour l'accès client. Il aborde les questions de sécurisation de l'environnement de messagerie, de déploiement de l'architecture serveur et de configuration des serveurs Exchange pour les méthodes d'accès client prises en charge.

Chapitre 3, « Gestion de l'accès client pour Exchange Server 2003 »
Ce chapitre décrit la gestion des paramètres d'accès client pour les protocoles et les clients pris en charge dans votre organisation.

Annexe, « Ressources »
Cette section contient des liens vers des ressources qui peuvent vous aider à mieux appréhender le fonctionnement des clients Exchange Server.

Configuration matérielle minimale requise

Pour exécuter les procédures décrites dans ce guide, vous devez disposer de la configuration matérielle ci-dessous. Cette liste ne comprend pas les serveurs Exchange, le matériel de stockage, etc. Elle ne comporte que le matériel nécessaire à la sécurité :

- Deux pare-feu (ou routeurs)
- Générateurs RSA SecurID PIN (pour chaque client mobile)
- Au minimum un serveur frontal exécutant Microsoft Internet Security and Acceleration Server (ISA)

Configuration logicielle

Pour exécuter les procédures décrites dans ce guide, vous devez disposer de la configuration logicielle suivante :

- Microsoft Exchange Server 2003 Enterprise Edition
- Microsoft ISA (Internet Security and Acceleration) Server
- Microsoft Windows 2000 Advanced Server
- RSA SecurID Server version 1.x

Présentation de Microsoft Exchange Server 2003 et de l'accès client

Exchange 2003 offre aux utilisateurs de nouvelles fonctionnalités pour la gestion de clients de messagerie. Exchange 2003 s'appuie sur les technologies des versions précédentes de Microsoft Exchange et les enrichit de plusieurs innovations en matière de messagerie. Nouveautés de Microsoft Exchange 2003 :

- Mode de mise en cache d'Outlook 2003
- Outlook 2003 utilisant RPC sur HTTP
- Prise en charge de périphériques mobiles via Outlook Mobile Access et ActiveSync Exchange
- Optimisation d'Outlook Web Access pour Exchange 2003

Grâce aux clients nouveaux et améliorés, vous pouvez proposer à vos utilisateurs un accès distant simplifié, des options d'accès supplémentaires et une expérience utilisateur plus enrichissante. Vous trouverez dans les sections suivantes un rapide tour d'horizon des clients nouveaux et améliorés ainsi que des technologies des clients de messagerie pour Exchange 2003.

Nouvelles fonctionnalités de Microsoft Exchange 2003 et Microsoft Outlook 2003

Les sections suivantes décrivent les nouvelles fonctionnalités de Microsoft Exchange 2003 et Microsoft Outlook 2003 qui simplifient les tâches de gestion de l'information et de la messagerie.

Accès à un serveur Exchange via Internet (RPC sur HTTP)

Outlook peut désormais se connecter à Exchange 2003 via Internet sans avoir à utiliser des connexions de type réseau privé virtuel (VPN, *Virtual Private Network*) lentes et pas toujours disponibles. Cette fonctionnalité vous permet d'accéder à votre compte Exchange 2003 à partir d'Internet lorsque vous travaillez au-delà du pare-feu de votre organisation sans disposer d'une connexion ou d'un matériel spécial, comme les cartes à puce ou les jetons de sécurité. Pour plus d'informations sur la configuration de Microsoft Exchange 2003 en vue d'une utilisation de RPC sur HTTP, consultez l'article (en anglais) *Exchange Server 2003 RPC over HTTP Deployment Scenarios* (http://go.microsoft.com/fwlink/?linkid=24823).

Améliorations de la synchronisation

Pour réduire la quantité d'informations échangées entre le client Outlook 2003 et les serveurs Exchange 2003, Exchange 2003 effectue une compression des données. Exchange 2003 réduit aussi le nombre global des demandes d'informations passées entre le client et le serveur, ce qui permet d'optimiser la communication entre ces deux entités.

Nouveau type de fichier de données (.pst)

Outlook introduit un nouveau format de fichier pour les fichiers de données personnels (.pst), qui offre une plus grande capacité pour les éléments et les dossiers tout en prenant en charge les données Unicode multilingues.

Remarque Les fichiers créés dans le nouveau format de fichier .pst d'Outlook ne sont pas compatibles avec les versions antérieures d'Outlook. Pour assurer la compatibilité avec les versions antérieures d'Outlook, créez des fichiers au format de fichier .pst pour Outlook 97 à Outlook 2002. Outlook 2003 peut afficher et créer des fichiers des deux types.

Protocole d'authentification Kerberos

Exchange 2003 permet aux clients Outlook 2003 de s'authentifier auprès des serveurs Exchange 2003 en utilisant l'authentification Kerberos.

Mode Exchange de mise en cache

L'ajout du mode Exchange de mise en cache, associé aux améliorations de la synchronisation et de l'optimisation, augmente considérablement les performances des utilisateurs finaux distants pour Outlook. Par exemple, dans les versions antérieures d'Outlook, les boîtes de dialogues affichaient les demandes d'informations à partir d'un serveur Exchange ; toutefois, dans Outlook 2003, ces demandes n'apparaissent plus sur le client Outlook d'un utilisateur, car celui-ci travaille principalement à partir de son fichier de données de boîte aux lettres Exchange local (cette fonctionnalité permet également de réduire la charge globale exercée sur vos serveurs Exchange). Plus important encore, si la connexion réseau est perdue entre le client Outlook et le réseau, Outlook 2003 n'interrompra pas son activité.

Améliorations liées à Outlook Web Access 2003

La nouvelle version d'Outlook Web Access dans Exchange 2003 contient des améliorations telles que l'authentification basée sur les formulaires, les règles, le correcteur orthographique et la possibilité d'envoyer et de recevoir des messages électroniques à signature numérique et cryptés. L'interface a été repensée pour offrir à l'utilisateur un cadre de travail similaire à celui présent dans Outlook 2003, avec un volet de lecture et un volet de navigation amélioré.

Outlook Web Access pour Exchange 2003 est plus rapide en particulier sur des connexions lentes et donc plus réactif aux interventions de l'utilisateur.

La liste suivante décrit brièvement quelques-unes des nouvelles fonctionnalités d'Outlook Web Access pour Exchange 2003 :

Octets transmis par câble

La réduction de la quantité d'informations à transférer du serveur au navigateur a permis une augmentation de la vitesse d'Outlook Web Access. Une quantité moindre d'octets est envoyée par câble du serveur au navigateur. Cependant, soyez conscient du fait que le processus de connexion utilise davantage d'octets que le processus de connexion dans Outlook 2003.

Prise en charge de la compression

Les administrateurs peuvent configurer la prise en charge de la compression pour Outlook Web Access, qui améliore les performances pour la plupart des actions sur les connexions réseau lentes. La compression Outlook Web Access permet de compresser les pages Web statiques et/ou dynamiques selon le paramètre de compression que vous utilisez. Vous pouvez activer la compression à partir du Gestionnaire système Exchange.

Authentification par formulaires

Vous pouvez activer une nouvelle page d'ouverture de session Outlook Web Access qui enregistre le nom et le mot de passe de l'utilisateur dans un cookie plutôt que dans le navigateur. Lorsque l'utilisateur ferme son navigateur, le cookie est supprimé. De plus, après un certain temps d'inactivité, le cookie est supprimé automatiquement. La nouvelle page d'ouverture de session nécessite que les utilisateurs entrent soit leur nom de domaine, nom d'utilisateur et leur mot de passe, soit leur adresse de messagerie UPN (User Principal Name) complète et leur mot de passe. Pour activer la page d'ouverture de session Outlook Web Access, vous devez activer l'authentification par formulaires sur le serveur.

Prise en charge du protocole de sécurité S/MIME

Le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions) améliore la sécurité des messages transmis sur Internet en permettant la signature numérique des messages, ainsi que leur cryptage. Les signatures numériques assurent l'authentification, la non-répudiation, ainsi que l'intégrité des données. Le cryptage des messages assure la confidentialité et l'intégrité des données.

Outlook Web Access pour Exchange 2000 ne prenait pas en charge les messages signés et cryptés. À présent, grâce au nouveau contrôle ActiveX® S/MIME Microsoft Outlook Web Access, les utilisateurs peuvent signer numériquement et crypter les messages électroniques. Le contrôle S/MIME fonctionne avec une infrastructure de clés publiques X.509 v3 quelconque pour fournir les fonctionnalités de signature et de cryptage.

Pour plus d'informations sur la prise en charge de S/MIME dans Outlook Web Access, consultez *Nouveautés d'Exchange 2003* (http://go.microsoft.com/fwlink/?linkid=21765).

Les améliorations apportées au niveau des caractéristiques, des fonctionnalités et des performances peuvent avoir une incidence sur le choix du client que vos utilisateurs doivent utiliser principalement pour accéder à leurs informations Exchange. Sur les sites distants, le choix prioritaire peut se porter sur Outlook Web Access qui est une possibilité à envisager lorsque vous planifiez des réseaux WAN et le placement des serveurs.

Prise en charge accrue du navigateur

Le tableau 1.1 montre le niveau de prise en charge du navigateur pour les systèmes d'exploitation compatibles avec Outlook Web Access pour Exchange 2003.

Tableau 1.1 Prise en charge du navigateur pour Outlook Web Access avec les systèmes d'exploitation Microsoft

	Windows 98 Deuxième Édition	Windows ME	Windows 2000	Windows XP	Windows Server 2003
Internet Explorer 5.1	B, P	Aucune	B, P	Aucune	Aucune
Internet Explorer 5.5 SP2	B, P	B, P	B, P	Aucune	Aucune
Internet Explorer 6	B, P	B, P	B, P	B, P	Aucune
Internet Explorer 6 SP1	B, P	B, P	B, P	B, P	B, P
MSN® version 8 et versions ultérieures	Aucune	Aucune	Aucune	B, P	B, P
Netscape Navigator 4.8	B	B	B	B	B
Netscape Navigator 7	B	B	B	B	B

Le tableau 1.2 indique le niveau de fonctionnalités pour les systèmes d'exploitation et les navigateurs d'Outlook Web Access.

Clé

- B - Version Basic d'Outlook Web Access prise en charge
- B,P - Les deux versions Basic et Premium d'Outlook Web Access sont prises en charge
- Aucune - Aucune des deux versions Basic et Premium d'Outlook Web Access n'est prise en charge

Tableau 1.2 Prise en charge du navigateur pour Outlook Web Access avec d'autres systèmes d'exploitation

	Apple OS 9.x	Apple OS 10.1 et versions ultérieures	Sun Microsystems Solaris HP / UX
Internet Explorer 5.0 et versions ultérieures pour	B	B	S/O

Apple			
Internet Explorer 5.5 SP2	Aucune	Aucune	Aucune
Internet Explorer 6	Aucune	Aucune	Aucune
Internet Explorer 6 SP1	Aucune	Aucune	Aucune
MSN version 8 et versions ultérieures	Aucune	Aucune	Aucune
Netscape Navigator 4.8	B	B	B
Netscape Navigator 6.2	B	B	B
Netscape Navigator 7	B	B	B

Clé

- B - Version Basic d'Outlook Web Access prise en charge
- B,P - Les deux versions Basic et Premium d'Outlook Web Access sont prises en charge
- Aucune - Aucune des deux versions Basic et Premium d'Outlook Web Access n'est prise en charge

Par ailleurs, la prise en charge des navigateurs et des systèmes d'exploitation suivants n'est plus assurée pour Exchange 2003 :

- Microsoft Internet Explorer 4.5
- Internet Explorer 5 sur toutes les versions de Microsoft Windows
- Internet Explorer 5 pour UNIX 6.0
- Internet Explorer 4.57 pour Apple OS 9 et versions ultérieures
- Microsoft Windows® 95
- Microsoft Windows® 98
- Microsoft Windows NT® 4.08
- Apple OS 8.17

Pour plus d'informations sur les nouvelles fonctionnalités d'Outlook Web Access, consultez *Nouveautés d'Exchange 2003* (http://go.microsoft.com/fwlink/?linkid=21765).

Services mobiles pour Exchange

Exchange Server 2003 prend en charge l'accès à distance en utilisant les capacités de synchronisation et de navigation des périphériques mobiles. Vous pouvez déployer des services mobiles pour permettre aux utilisateurs d'accéder à leurs informations Exchange à partir de périphériques mobiles, tels que le périphérique Microsoft Pocket PC 2002 Phone Edition, ou d'un périphérique mobile quelconque doté d'un navigateur mobile.

ActiveSync Exchange

Exchange 2003 peut à présent utiliser les périphériques Pocket PC 2002 pour synchroniser les données Exchange avec ActiveSync® Exchange. Par défaut, lorsque vous installez Exchange, tous vos utilisateurs sont configurés pour la synchronisation.

En synchronisant un périphérique avec un serveur Exchange, vos utilisateurs peuvent accéder à leurs informations Exchange sans avoir à être toujours connectés à un réseau mobile. En particulier, les utilisateurs peuvent utiliser leur connexion d'opérateur mobile pour synchroniser leurs informations Exchange sur leur périphérique Pocket PC Phone Edition ou Smartphone, puis accéder à ces informations en mode hors connexion.

Outlook Mobile Access

Exchange 2003 inclut à présent l'application Outlook Mobile Access, qui permet aux utilisateurs d'utiliser des périphériques mobiles pour accéder à leurs dossiers de messagerie, Contacts, Calendrier et Tâches. Outlook Mobile Access peut être utilisé avec un périphérique mobile doté d'un navigateur mobile. Le navigateur mobile doit prendre en charge un des langages de balisage suivants : HTML, xHTML ou cHTML. Pour déployer votre serveur Exchange et utiliser Outlook Mobile Access, suivez la même procédure que celle qui consiste à déployer un serveur Exchange pour utiliser Outlook Web Access.

Présentation des besoins de sécurité d'Outlook Mobile Access

Lorsque vous activez Outlook Mobile Access pour vos utilisateurs, un problème de sécurité se pose pour les opérateurs mobiles utilisant des passerelles WAP (Wireless Application Protocol) 1.x. Ces passerelles convertissent le trafic sécurisé entre les protocoles Internet et les protocoles sans fil. En raison de cette conversion, une passerelle WAP 1.x termine une session SSL sur TCP/IP, recrypte les données en appliquant WTLS (Wireless Transport Layer Security), puis envoie les informations via le réseau sans fil par l'intermédiaire du protocole WSP (Wireless Session Protocol). Lors de cette opération de conversion au niveau de la passerelle WAP, toutes les données se retrouvent temporairement non cryptées, dans la mesure où elles sont décryptées après la session SSL avant d'être recryptées pour la session WTLS. Ce problème de sécurité affecte votre infrastructure de messagerie si votre société n'héberge pas sa propre passerelle WAP dans le réseau de périmètre.

Outlook Mobile Access pour Exchange 2003 prend uniquement en charge les périphériques WAP 2.0. Cependant, cela n'exclut nullement la possibilité pour certains périphériques d'utiliser une passerelle WAP 1.x. Par conséquent, le problème de sécurité existe chaque fois qu'un périphérique WAP 2.0, pouvant utiliser une passerelle WAP 1.x, utilise un opérateur mobile ayant des passerelles WAP 1.x déployées.

Pour résoudre ce problème, vous pouvez acheter et installer votre propre passerelle WAP d'entreprise. Cette solution vous oblige à implanter une passerelle WAP dans les limites de votre réseau de périmètre et d'imposer aux utilisateurs itinérants l'utilisation de cette seule passerelle.

Vous pouvez également choisir de fournir uniquement des périphériques WAP 2.0 qui utilisent exclusivement des opérateurs ayant déployé des passerelles WAP 2.0. Les passerelles WAP 2.0 autorisent des sessions SSL directes avec les périphériques WAP 2.0 compatibles SSL, sans décryptage puis recryptage de la session.

Planification d'une infrastructure d'accès client pour Exchange

Pour planifier votre infrastructure d'accès client pour Exchange, vous devez d'abord identifier la configuration technique requise pour votre système de messagerie Exchange. Une fois les besoins techniques identifiés, vous pouvez effectuer une analyse des écarts afin de déterminer quelles sont les modifications à apporter à votre environnement actuel, y compris les mises à niveau de l'infrastructure réseau, des composants matériels et des logiciels. De plus, vous devez parfaitement appréhender la teneur des concepts de base qui sous-tendent les facteurs à prendre en compte lors de la planification de votre infrastructure Exchange. Certains de ces facteurs sont répertoriés ci-dessous :

- Sécurité
- Frontières et limites topologiques
- Systèmes de messagerie centralisés ou systèmes de messagerie distribués
- Conception du routage
- Conception et placement des serveurs
- Dimensionnement et réglage du serveur

- Besoins des utilisateurs

Tous ces facteurs vous aident à concevoir l'infrastructure d'accès client nécessaire pour répondre à vos besoins de messagerie. Pour plus d'informations sur la conception et la planification de vos systèmes de messagerie, consultez *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766).

Configuration de Microsoft Exchange Server 2003 pour l'accès client

Ce chapitre fournit des informations sur la configuration des fonctionnalités Microsoft Exchange Server 2003 pour l'accès client. Avant de déployer les fonctionnalités d'accès client, prenez le temps d'examiner les répercussions que ces fonctionnalités peuvent avoir sur votre environnement de messagerie. De plus, le déploiement de fonctionnalités client pour Exchange 2003 implique les activités suivantes :

- sécurisation de votre environnement de messagerie Exchange ;
- déploiement de votre architecture serveur ;
- configuration des serveurs Exchange pour vos méthodes d'accès client prises en charge.

Sécurisation de votre environnement de messagerie Exchange

Pour sécuriser votre environnement de messagerie Exchange, suivez ces étapes :

1. Mettre à jour votre logiciel serveur.
2. Sécuriser l'environnement de messagerie.
3. Sécuriser les communications.

Pour sécuriser votre système de messagerie, exécutez ces étapes dans l'ordre indiqué.

Mise à jour de votre logiciel serveur

Après avoir installé Exchange 2003, vous devez mettre à jour le logiciel serveur sur vos serveurs Exchange et sur tous les autres serveurs avec lesquels Exchange communique, tels que les serveurs de catalogue global et contrôleurs de domaine. Pour plus d'informations sur la mise à jour de votre logiciel avec les dernières mises à jour de sécurité, consultez le site Web du Centre de sécurité Microsoft Exchange Server (http://go.microsoft.com/fwlink/?linkid=18412). Pour plus d'informations sur la sécurité Microsoft, consultez le site Web de sécurité Microsoft (http://go.microsoft.com/fwlink/?linkid=21633).

Sécurisation de l'environnement de messagerie Exchange

Si vous ne pouvez pas placer vos serveurs frontaux Exchange 2003 à l'intérieur du réseau de périmètre, il est préconisé de déployer Microsoft ISA (Internet Security and Acceleration) Server 2000. ISA Server joue le rôle de pare-feu avancés qui contrôlent le trafic Internet entrant dans votre réseau. Lorsque vous utilisez cette configuration, vous placez tous les serveurs Exchange 2003 à l'intérieur du réseau d'entreprise et utilisez ISA Server comme serveur pare-feu avancé, exposé au trafic Internet dans votre réseau de périmètre.

La sécurisation de l'environnement de messagerie requiert également la configuration des serveurs frontaux de manière à désactiver les fonctionnalités et les paramètres de serveur frontal qui ne sont pas nécessaires dans une architecture de serveurs frontaux et principaux. Pour plus d'informations sur la configuration d'un serveur frontal pour l'architecture serveur frontal/principal, consultez *Using Microsoft Exchange 2000 Front-end Servers* (en anglais) (http://go.microsoft.com/fwlink/?linkid=12055).

L'ensemble du trafic Internet entrant en direction des serveurs Exchange, par exemple, Outlook Web Access, les communications RPC sur HTTP en provenance de clients Outlook 2003, Outlook Mobile Access, POP3

(Post Office Protocol version 3), IMAP4 (Internet Message Access Protocol version 4rev1), etc., est traité par le serveur ISA. Lorsqu'ISA Server reçoit une demande d'accès à un serveur Exchange, il traite les demandes par procuration sur les serveurs Exchange de votre réseau interne. Les serveurs Exchange internes renvoient les données demandées au serveur ISA qui transmet ensuite les informations au client via Internet. La figure 2.1 illustre un exemple de déploiement ISA Server recommandé.

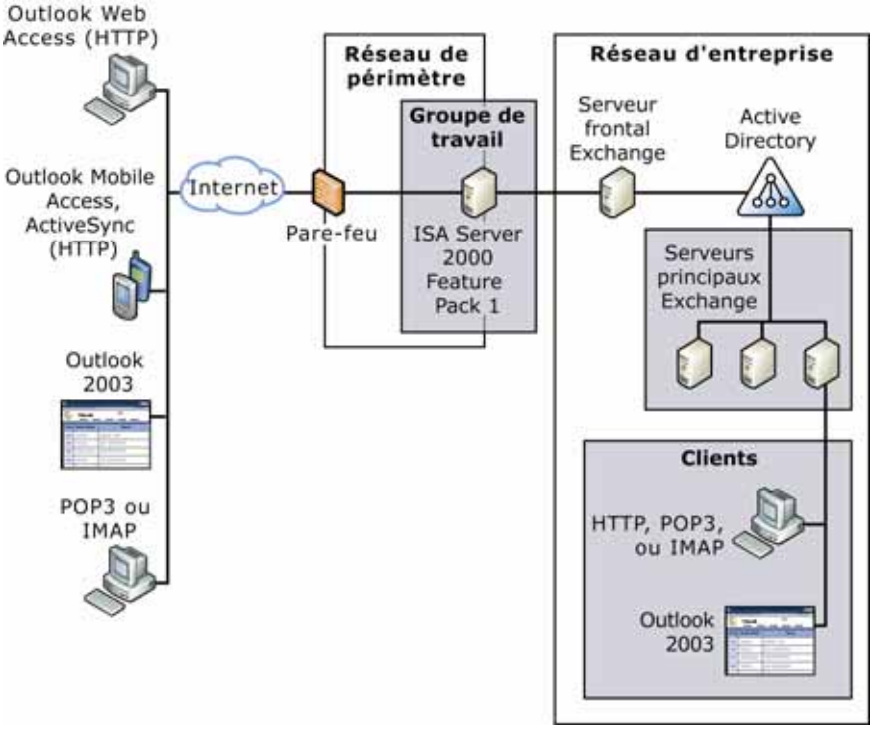

Figure 2.1 Déploiement de Microsoft Exchange 2003 derrière ISA Server

Sécurisation des communications

Pour sécuriser les communications dans votre environnement de messagerie Exchange, vous devez effectuer les tâches suivantes :

- sécuriser les communications entre les applications de messagerie clientes et le serveur frontal Exchange ;
- sécuriser les communications entre le serveur frontal Exchange et le réseau interne.

Les sections suivantes contiennent des informations relatives à la sécurisation des communications pour ces deux cas de figure.

Sécurisation des communications entre le client et le serveur frontal Exchange

Pour sécuriser les données échangées entre le client et le serveur frontal, il est fortement recommandé d'activer le serveur frontal pour utiliser SSL (Secure Sockets Layer). En outre, pour garantir que les données de l'utilisateur sont toujours sécurisées, vous devez configurer le serveur frontal pour qu'il exige SSL. (Cette option peut être définie dans la configuration SSL.) Lorsque l'authentification de base est utilisée, il est essentiel de protéger le trafic réseau à l'aide de SSL afin de protéger les mots de passe des utilisateurs contre le repérage de paquets sur le réseau.

> **Avertissement** Si vous n'utilisez pas SSL entre les clients et le serveur frontal, la transmission de données HTTP à votre serveur frontal ne sera pas sécurisée. Il est fortement recommandé de configurer le serveur frontal pour qu'il requière SSL.

Nous vous conseillons de vous procurer un certificat SSL en achetant un certificat à une Autorité de certification (CA, *Certification Authority*) tierce. L'achat d'un certificat auprès d'une Autorité de certification est la méthode privilégiée car la plupart des navigateurs approuvent un grand nombre de ces Autorités de certification.

Vous pouvez également utiliser les services de certificats pour installer vos propres Autorités de certification. Bien que l'installation de votre propre Autorité de certification puisse être moins coûteuse, les navigateurs n'approuveront pas votre certificat, et les utilisateurs recevront un message d'avertissement indiquant que le certificat n'est pas approuvé. Pour plus d'informations sur SSL, consultez l'article 320291 de la Base de connaissances Microsoft, « XCCC : Activation de SSL pour Exchange 2000 Server Outlook Web Access » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=320291).

Utilisation de SSL (Secure Sockets Layer)

Pour protéger les messages sortants et entrants, déployez SSL pour crypter le trafic de messagerie. Vous pouvez configurer les fonctionnalités de sécurité SSL sur un serveur Exchange pour vérifier l'intégrité de votre contenu, vérifier l'identité des utilisateurs et crypter les transmissions réseau. Exchange, comme tout serveur Web, requiert un certificat de serveur valide pour établir des communications SSL. Vous pouvez utiliser l'Assistant Certificat de serveur Web pour générer un fichier de demande de certificat (par défaut, NewKeyRq.txt) que vous pouvez envoyer à une Autorité de certification, ou générer une demande d'Autorité de certification en ligne, telle que les services de certificats Microsoft.

Si vous n'utilisez pas les services de certificats pour émettre vos propres certificats de serveur, une Autorité de certification tierce doit approuver votre demande et émettre votre certificat de serveur. Pour plus d'informations sur les certificats de serveur, consultez « Obtention et installation de certificats de serveur », plus loin dans ce chapitre. En fonction du niveau d'assurance d'identification proposé par votre certificat de serveur, l'approbation de votre demande et l'envoi de votre fichier de certificat par l'Autorité de certification peut demander de plusieurs jours à plusieurs mois. Vous ne pouvez avoir qu'un seul certificat de serveur pour chaque site Web.

Une fois que vous avez reçu un fichier de certificat de serveur, utilisez l'Assistant Certificat de serveur Web pour l'installer. Le processus d'installation attache (ou lie) votre certificat à un site Web.

> **Important** Pour exécuter la procédure suivante, vous devez être membre du groupe Administrateurs sur l'ordinateur local, ou bien l'autorité appropriée doit vous avoir été déléguée. En matière de sécurité, il est préconisé de se connecter à l'ordinateur en utilisant un compte qui ne figure pas dans le groupe Administrateurs, puis d'utiliser la commande **Exécuter en tant que** pour exécuter le Gestionnaire des services Internet en tant qu'administrateur. À l'invite de commandes, tapez la commande suivante :
>
> ```
> runas /utilisateur:nom_compte_administration
> "mmc%systemroot%\system32\inetsrv\iis.msc"
> ```

Pour configurer SSL sur un serveur

1. Dans le Gestionnaire des services Internet, développez l'ordinateur local, puis le dossier **Sites Web**. Cliquez avec le bouton droit sur le site Web ou le fichier que vous voulez protéger avec SSL, puis cliquez sur **Propriétés**.
2. Sous **Identification de site Web**, cliquez sur **Avancé**.
3. Dans la zone **Identification avancée de site Web**, sous **Identités multiples pour ce site Web**, vérifiez que l'adresse IP du site Web est affectée au port 443 (port par défaut pour les communications sécurisées), puis cliquez sur **OK**. Facultativement, pour configurer d'autres ports SSL pour ce site Web, cliquez sur **Ajouter** sous **Identités multiples pour ce site Web**, puis cliquez sur **OK**.
4. Sous l'onglet **Sécurité de répertoire**, sous **Communications sécurisées**, cliquez sur **Modifier**.
5. Dans la boîte **Communications sécurisées**, activez la case à cocher **Requérir un canal sécurisé (SSL)**.

Si l'utilisation du cryptage de clés sur 128 bits est requise, vos utilisateurs doivent utiliser des navigateurs Web qui prennent en charge le cryptage sur 128 bits. Pour plus d'informations sur la mise à niveau vers le cryptage 128 bits, visitez le site Web du service de Support technique Microsoft (http://go.microsoft.com/fwlink/?linkid=14898).

Obtention et installation de certificats de serveur

Vous pouvez obtenir des certificats de serveur auprès d'une Autorité de certification (CA) externe, ou émettre vos propres certificats de serveur à l'aide des services de certificats Microsoft. Une fois que vous avez obtenu un certificat de serveur, vous pouvez l'installer. Lorsque vous utilisez l'Assistant Certificat de serveur Web pour obtenir et installer un certificat de serveur, le processus correspond à la création et à l'affectation d'un certificat de serveur.

Cette section décrit les problèmes à prendre en considération avant de prendre la décision d'obtenir vos certificats de serveur auprès d'une Autorité de certification extérieure ou d'émettre vos propres certificats de serveur. Elle comprend les informations suivantes :

- Obtention de certificats de serveur auprès d'une Autorité de certification
- Émission de vos propres certificats de serveur
- Installation de certificats de serveur
- Sauvegarde de certificats de serveur

Obtention de certificats de serveur d'une Autorité de certification

Si vous remplacez votre certificat de serveur actuel, IIS continue à utiliser ce certificat jusqu'à ce que la nouvelle demande soit terminée. Lorsque vous sélectionnez une Autorité de certification, prenez en considération les questions suivantes :

- L'Autorité de certification pourra-t-elle émettre un certificat compatible avec l'ensemble des navigateurs utilisés pour accéder à mon serveur ?
- L'Autorité de certification est-elle une organisation reconnue et approuvée ?
- Comment l'Autorité de certification vérifiera-t-elle mon identité ?
- L'Autorité de certification dispose-t-elle d'un système pour recevoir des demandes de certificats en ligne, telles que celles générées par l'Assistant Certificat de serveur Web ?
- Combien coûtera initialement le certificat, et combien coûteront le renouvellement ou les autres services ?
- L'Autorité de certification connaît-elle les intérêts commerciaux de mon organisation ou de mon entreprise ?

Pour obtenir un certificat de serveur d'une Autorité de certification

1. Utilisez l'Assistant Certificat de serveur Web pour créer une demande de certificat.
2. Dans l'Assistant Certificat de serveur Web, à la page **Demande ultérieure ou immédiate**, cliquez sur **Préparer la demande, mais ne pas l'envoyer maintenant**.
3. Utilisez l'Assistant Certificat de serveur Web pour envoyer la demande à l'Autorité de certification. L'Autorité de certification traitera la demande, puis vous enverra le certificat.
4. Mettez fin à l'utilisation de l'Assistant Certificat de serveur Web.

   Remarque Certaines Autorités de certification vous demandent de prouver votre identité avant de traiter votre demander ou d'émettre un certificat.

Émission de vos propres certificats de serveur

Avant de prendre la décision d'émettre vos propres certificats de serveur, prenez en considération les points suivants :

- Sachez que les services de certificats Microsoft gèrent différents formats de certificats et permettent l'audit et l'enregistrement de l'activité liée aux certificats.
- Comparez le coût d'émission de vos propres certificats avec le coût d'achat d'un certificat à une Autorité de certification.
- Gardez à l'esprit que votre organisation nécessitera une période d'ajustement initiale pour connaître, implémenter et intégrer les services de certificats aux systèmes et stratégies de sécurité existants.

- Évaluez la volonté de vos clients qui se connectent à approuver votre organisation en tant que fournisseur de certificats.

Utilisez les services de certificats pour créer un service personnalisable pour l'émission et la gestion de certificats. Vous pouvez créer des certificats de serveur pour Internet ou pour des intranets d'entreprise, et donner ainsi à votre organisation le contrôle total sur les stratégies de gestion des certificats. Pour plus d'informations sur l'utilisation des services de certificats, consultez « Services de certificats » dans l'aide de Microsoft Windows Server 2003.

Les demandes en ligne de certificats de serveur ne peuvent être présentées qu'à des services de certificats d'entreprise locaux et distants, ainsi qu'à des services de certificats autonomes distants. L'Assistant Certificat de serveur Web ne reconnaît pas une installation autonome des services de certificats sur le même ordinateur lors de la demande d'un certificat. Si vous devez utiliser l'Assistant Certificat de serveur Web sur le même ordinateur qu'une installation des services de certificats autonomes, utilisez la demande de certificat en ligne pour enregistrer la demande dans un fichier, puis traitez-la comme une demande en mode hors connexion. Pour plus d'informations sur l'utilisation des services de certificats, consultez « Services de certificats » dans l'aide de Microsoft Windows Server 2003.

Remarque Si vous ouvrez un certificat SGC (Server Gated Cryptography), vous pouvez recevoir l'avis suivant sous l'onglet **Général** :

```
The certificate has failed to verify for all its intended purposes.
```

Cette mention est émise en raison de la façon dont les certificats SGC interagissent avec Windows et n'indique pas nécessairement que le certificat ne fonctionne pas correctement.

Installation de certificats de serveur

Après avoir obtenu un certificat de serveur auprès d'une Autorité de certification, ou après avoir émis votre propre certificat de serveur à l'aide des services de certificats, utilisez l'Assistant Certificat de serveur Web pour l'installer.

Sauvegarde de certificats de serveur

Vous pouvez utiliser l'Assistant Certificat de serveur Web pour sauvegarder des certificats de serveur. Étant donné qu'IIS fonctionne de façon étroite avec Windows, vous pouvez utiliser le Gestionnaire de certificats, qui est appelé **Certificats** dans Microsoft Management Console (MMC), pour exporter et sauvegarder vos certificats de serveur.

Remarque Si le Gestionnaire de certificats n'est pas installé dans MMC, utilisez la procédure **Pour ajouter le Gestionnaire de certificats à MMC** ci-dessous pour l'ajouter.

Pour ajouter le Gestionnaire de certificats à MMC

1. Cliquez sur **Démarrer**, puis sur **Exécuter**.
2. Dans la zone **Ouvrir**, tapez **mmc**, puis cliquez sur **OK**.
3. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la zone **Ajouter/Supprimer un composant logiciel enfichable**, cliquez sur **Ajouter**.
5. Dans la liste **Composants logiciels enfichables disponibles**, cliquez sur **Certificats**, puis sur **Ajouter**.
6. Cliquez sur **Le compte de l'ordinateur**, puis sur **Suivant**.
7. Cliquez sur l'option **L'ordinateur local** (l'ordinateur sur lequel cette console s'exécute), puis sur **Terminer**.
8. Cliquez sur **Fermer**, puis sur **OK**.

Après avoir installé le Gestionnaire de certificats, vous pouvez sauvegarder votre certificat.

Pour sauvegarder votre certificat de serveur

1. Localisez le magasin de certificats approprié. Il s'agit généralement du magasin **Ordinateur local** du Gestionnaire de certificats.

Remarque Une fois le Gestionnaire de certificats installé, il pointe vers le magasin de certificats **Ordinateur local** approprié.

2. Dans le magasin **Personnel**, cliquez sur le certificat que vous voulez sauvegarder.
3. Dans le menu **Action**, pointez sur **Toutes les tâches**, puis cliquez sur **Exporter**.
4. Dans l'Assistant Exportation de certificat, cliquez sur **Oui, exporter la clé privée**.
5. Suivez les paramètres par défaut de l'Assistant, puis entrez un mot de passe pour le fichier de sauvegarde de certificat lorsque vous y êtes invité.

   Remarque Ne sélectionnez pas **Supprimer la clé privée si l'exportation s'est terminée correctement** car cette option désactive votre certificat de serveur actuel.
6. Exécutez l'Assistant pour exporter une copie de sauvegarde de votre certificat de serveur.

Après avoir configuré votre réseau pour émettre des certificats de serveur, vous devez sécuriser votre serveur frontal Exchange et les services de votre serveur Exchange en demandant la communication SSL avec le serveur frontal Exchange. La section suivante explique comment activer SSL pour votre site Web par défaut.

Activation de SSL pour le site Web par défaut

Après avoir obtenu un certificat SSL à utiliser avec votre serveur frontal Exchange sur le site Web par défaut ou sur le site sur lequel vous hébergez les répertoires virtuels \RPC, \OMA, \Microsoft-Server-ActiveSync, \Exchange, \Exchweb et \Public, vous pouvez activer le site Web par défaut pour qu'il exige SSL.

Remarque Les répertoires virtuels \Exchange, \Exchweb, \Public, \OMA et \Microsoft-Server-ActiveSync sont installés par défaut lors de toute installation Exchange 2003. Le répertoire virtuel \RPC pour la communication RPC sur HTTP est installé manuellement lorsque vous configurez Exchange pour qu'il prenne en charge RPC sur HTTP. Pour plus d'informations sur la configuration de Microsoft Exchange pour qu'il utilise RPC sur HTTP, consultez « Configuration de RPC sur HTTP pour Outlook 2003 », plus loin dans ce chapitre.

Pour configurer des répertoires virtuels en vue de l'utilisation de SSL

1. Dans **Services Internet (IIS)**, sélectionnez **Site Web par défaut** ou le site Web sur lequel vous hébergez vos services Exchange, puis cliquez sur **Propriétés**.
2. Sous l'onglet **Sécurité de répertoire**, dans **Communications sécurisées**, cliquez sur **Modifier**.
3. Dans **Communications sécurisées**, activez la case à cocher **Requérir un canal sécurisé (SSL)**.
4. Une fois cette procédure exécutée, tous les répertoires virtuels se trouvant sur le serveur frontal Exchange du site Web par défaut sont configurés pour utiliser SSL.

Sécurisation des communications entre le serveur frontal Exchange et d'autres serveurs

Après avoir sécurisé vos communications entre les ordinateurs clients et les serveurs frontaux Exchange, vous devez sécuriser les communications entre le serveur Exchange et les autres serveurs de votre organisation. Les communications HTTP, POP et IMAP entre le serveur frontal et tout serveur avec lequel le serveur frontal communique (par exemple, les serveurs principaux, les contrôleurs de domaine et les serveurs de catalogue global) ne sont pas cryptées. Lorsque le serveur frontal et les serveurs principaux se trouvent dans un réseau physique ou commuté approuvé, ce manque de cryptage n'est pas inquiétant. Toutefois, si le serveur frontal et les serveurs principaux sont conservés dans des sous-réseaux distincts, le trafic réseau peut transiter par des zones non sécurisées du réseau. Le risque pour la sécurité est plus important lorsque la distance physique entre le serveur frontal et les serveurs principaux augmente. Dans ce cas, il est conseillé que ce trafic soit crypté pour protéger les mots de passe et les données.

Utilisation d'IPSec pour crypter le trafic IP

Windows 2000 prend en charge la sécurité du protocole Internet (IPSec, *Internet Protocol security*), norme Internet qui permet à un serveur de crypter tout trafic IP, excepté le trafic qui utilise des adresses de diffusion ou des adresses IP de multidiffusion. En général, vous utilisez IPSec pour crypter le trafic HTTP ; toutefois, vous pouvez également utiliser IPSec pour crypter le trafic LDAP (Lightweight Directory Access Protocol), RPC, POP et IMAP. IPSec vous permet d'effectuer les opérations suivantes :

- configurer deux serveurs exécutant Windows 2000 pour requérir l'accès réseau approuvé ;
- transférer des données protégées contre la modification (à l'aide d'un total de contrôle cryptographique sur chaque paquet) ;
- crypter tout trafic entre deux serveurs au niveau de la couche IP.

Dans une topologie frontale/principale, vous pouvez utiliser IPSec pour crypter le trafic entre le serveur frontal et les serveurs principaux qui, sans cela, ne serait pas crypté. Pour plus d'informations sur la configuration d'IPSec avec des pare-feu, consultez l'article 233256 en anglais de la Base de connaissances Microsoft, « How to Enable IPSec Traffic Through a Firewall » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=233256).

Déploiement de l'architecture Exchange Server

Après avoir sécurisé votre environnement de messagerie Exchange, vous pouvez déployer l'architecture serveur frontal/principal Exchange. Pour plus d'informations sur l'architecture serveur frontal/principal Exchange, consultez la section « Protocoles » du manuel *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766).

Pour configurer l'architecture serveur frontal/principal Exchange, vous devez configurer un serveur Exchange en tant que serveur frontal. Avant de poursuivre le processus d'installation, veillez à passer en revue vos options de déploiement. La section suivante vous aide dans votre décision de déployer Exchange 2003 dans une configuration de serveur frontal/principal.

Une configuration frontale/principale est recommandée pour les organisations qui comportent plusieurs serveurs et utilisent Outlook Web Access, POP ou IMAP, ainsi que pour les organisations qui souhaitent fournir un accès HTTP, POP ou IMAP à leurs employés.

Configuration d'un serveur frontal

Un serveur frontal est un serveur Exchange ordinaire jusqu'à ce qu'il soit configuré en comme tel. Un serveur frontal ne doit héberger aucun utilisateur ni aucun dossier public, et doit être membre de la même organisation Exchange 2003 que les serveurs principaux (et donc être membre de la même forêt Windows 2000 Server ou Windows Server 2003). Les serveurs exécutant soit Exchange Server 2003 Édition Entreprise soit Exchange Server 2003 Édition Standard peuvent être configurés comme serveurs frontaux.

Pour désigner un serveur frontal

1. Démarrez le Gestionnaire système Exchange.
2. Dans l'arborescence de la console, développez **Serveurs**, cliquez avec le bouton droit sur le serveur que vous voulez désigner comme serveur frontal, puis cliquez sur **Propriétés**.
3. Dans **Propriétés de *Nom_serveur***, sous l'onglet **Général**, activez la case à cocher **Serveur frontal**.
4. Cliquez sur **Appliquer**, puis sur **OK**.

Pour commencer à utiliser votre serveur en tant que serveur frontal, redémarrez le serveur. Pour plus d'informations sur les scénarios, les configurations et l'installation des serveurs frontaux et principaux, consultez les manuels suivants :

- *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766)

- *Using Microsoft Exchange 2000 Front-End Servers* (en anglais) (http://go.microsoft.com/fwlink/?linkid=12055).

Configuration de Microsoft Exchange pour l'accès client

La configuration de Microsoft Exchange pour l'accès client implique la configuration de Microsoft Exchange pour traiter les protocoles et les clients que vous voulez prendre en charge. La section suivante explique comment activer les protocoles clients pris en charge par Exchange sur le serveur Exchange. Cette section comprend les parties suivantes :

- Configuration des fonctionnalités d'Outlook 2003
- Configuration de la prise en charge des périphériques mobiles
- Configuration d'Outlook Web Access
- Activation des serveurs virtuels POP3 et IMAP4

Configuration des fonctionnalités d'Outlook 2003

Outlook 2003 vous permet d'utiliser la fonctionnalité Windows RPC sur HTTP pour fournir un accès distant à Exchange pour tous vos utilisateurs. Avec le mode Exchange de mise en cache, qui permet aux utilisateurs d'utiliser une copie de leur boîte aux lettres Exchange sur leur ordinateur local, vos utilisateurs pourront accéder à Exchange à partir d'un environnement dans lequel la connectivité réseau est lente, fluctuante ou non existante. Les sections suivantes décrivent la façon de configurer Exchange pour tirer parti de ces fonctionnalités.

Configuration de RPC sur HTTP pour Outlook 2003

Le déploiement de RPC sur HTTP pour la prise en charge des clients Outlook 2003 pour l'accès distant à Exchange exige que vous suiviez attentivement les étapes nécessaires au déploiement de cette fonctionnalité. Pour plus d'informations sur le déploiement de cette fonctionnalité et la configuration des utilisateurs à l'aide d'Outlook 2003, consultez *Exchange Server 2003 RPC over HTTP Deployment Scenarios* (http://go.microsoft.com/fwlink/?linkid=24823).

Configuration de la prise en charge des périphériques mobiles

Effectuez les activités suivantes pour configurer la prise en charge des périphériques mobiles pour Exchange 2003 :

- Configuration de la synchronisation
- Configuration d'ActiveSync Exchange pour utiliser RSA SecurID
- Activation d'Outlook Mobile Access

Configuration de la synchronisation

Lorsque vous installez Exchange, l'accès à la synchronisation dans Exchange est activée par défaut pour tous les utilisateurs de l'organisation. Vous pouvez également utiliser le composant enfichable Utilisateurs et ordinateurs Active Directory pour activer l'accès à la synchronisation pour des utilisateurs individuels.

Configuration d'ActiveSync Exchange

La procédure ci-après vous explique comment configurer ActiveSync Exchange dans votre organisation.

Pour configurer votre organisation Exchange 2003 pour ActiveSync Exchange

1. Démarrez le Gestionnaire système Exchange.
2. Développez l'option **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. Sous **ActiveSync Exchange**, activez les cases à cocher de votre choix parmi les suivantes :
   - Activez la case à cocher **Activer la synchronisation initiée par l'utilisateur** pour autoriser les utilisateurs à utiliser des périphériques Pocket PC 2002 pour synchroniser leurs données Exchange.
   - Activez la case à cocher **Activer les notifications actualisées** pour permettre aux utilisateurs de recevoir des notifications, qui sont envoyées à partir du serveur Exchange vers des périphériques qui autorisent les notifications.
   - Activez la case à cocher **Activer les notifications aux adresses SMTP spécifiées par l'utilisateur** pour permettre aux utilisateurs d'utiliser leur propre opérateur SMTP pour les notifications.

     Remarque Une fois cette fonctionnalité activée, lorsqu'un nouveau message arrive dans la boîte aux lettres d'un utilisateur, les notifications actualisées permettent l'exécution d'une synchronisation sur un périphérique de l'utilisateur. Activez cette fonctionnalité si certains de vos utilisateurs utilisent des périphériques mobiles pour la synchronisation et que vous ne voulez pas spécifier l'opérateur.
4. Cliquez sur **Appliquer**, puis sur **OK**.

La procédure ci-après vous explique comment configurer un périphérique mobile, tel qu'un périphérique Pocket PC Phone Edition, pour utiliser ActiveSync Exchange. Exécutez cette procédure sur chaque périphérique mobile de votre organisation. Au lieu de cela, vous pouvez apprendre à vos utilisateurs à configurer leurs propres périphériques.

Pour configurer les périphériques Pocket PC Phone Edition afin qu'ils utilisent ActiveSync Exchange

1. Sur le périphérique mobile, sur l'écran Aujourd'hui, appuyez sur **Démarrer** puis sur **ActiveSync**.
2. Tapez sur **Outils**, sur **Options**, puis tapez sur l'onglet **Serveur**.
3. Activez la case à cocher en regard de chaque type d'informations que vous voulez synchroniser avec le serveur.
4. Pour configurer des options de synchronisation pour chaque type d'informations, sélectionnez le type d'informations, puis tapez sur **Paramètres**.
5. Dans le champ **Nom de serveur**, entrez l'adresse ou le nom du serveur auquel vous voulez vous connecter lors de la synchronisation des données Exchange.
6. Tapez sur **Avancé**.
7. Sous l'onglet **Connexion**, entrez le nom d'utilisateur, le mot de passe et le nom de domaine.
8. Dans l'onglet **Règles**, sélectionnez la règle qui vous convient le mieux, concernant la manière dont la synchronisation doit fonctionner lorsque des informations sont modifiées sur votre périphérique et sur votre serveur Exchange.
9. Tapez sur **OK** pour accepter les modifications que vous avez apportées à ActiveSync.
10. Répétez cette procédure pour chacun des périphériques Pocket PC Phone Edition de vos utilisateurs. Au lieu de cela, vous pouvez apprendre à vos utilisateurs à configurer eux-mêmes leurs périphériques en vue d'une utilisation avec ActiveSync Exchange.

Configuration d'ActiveSync Exchange pour utiliser RSA SecurID

Pour disposer d'une couche de sécurité supplémentaire, vous pouvez utiliser les périphériques Microsoft Windows Mobile avec ActiveSync Exchange et l'authentification à deux facteurs de RSA SecurID.

> **Remarque** La prise en charge de RSA SecurID ne nécessite aucune configuration de périphérique supplémentaire. Le périphérique présente automatiquement l'authentification appropriée lors de la synchronisation avec un serveur Exchange ActiveSync protégé par RSA SecurID.

Suivez ces étapes pour utiliser RSA SecurID avec ActiveSync Exchange :

1. Configuration des composants de serveur RSA SecurID.
2. Configuration des services Internet (IIS) pour utiliser RSA SecurID
3. Installation des comptes d'utilisateur.

Configuration des composants de serveur RSA SecurID.

Pour configurer les composants serveur RSA SecurID, vous devez :

- **configurer le composant RSA ACE/Server** Le composant RSA ACE/Server est le serveur RSA qui enregistre et gère les informations et tickets d'authentification de vos utilisateurs. Pour configurer le composant RSA ACE/Server, suivez les procédures décrites dans la documentation RSA SecurID fournie par RSA Security Inc.
- **configurer le composant RSA ACE/Agent sur le serveur frontal** le composant RSA ACE/Agent est le filtre ISAPI (Internet Server Application Programming Interface) qui effectue l'authentification et communique avec le composant ACE/Server pour récupérer les informations d'authentification SecurID. Pour configurer le composant RSA ACE/Agent, suivez les procédures décrites dans la documentation RSA fournie par RSA Security Inc.

Configuration des services Internet pour utiliser RSA SecurID

Exécutez les procédures suivantes pour configurer les services Internet pour RSA et ActiveSync Exchange :

1. Protection des répertoires virtuels ActiveSync Exchange ActiveSync.
2. Personnalisation de l'en-tête de réponse HTTP pour les périphériques.
3. Installation des écrans SecurID (facultatif). Pour plus d'informations sur l'installation de ces écrans, consultez la documentation RSA SecurID fournie par RSA Security Inc.

Les sections suivantes contiennent des informations sur l'exécution de ces étapes pour configurer correctement les services Internet pour les opérations SecurID et Active Exchange.

Protection des répertoires virtuels ActiveSync Exchange

La première étape de la configuration des services Internet consiste à protéger les répertoires virtuels auxquels vos utilisateurs accèdent lorsqu'ils utilisent ActiveSync Exchange. Exchange Server 2003 utilise le répertoire virtuel \Microsoft-Server-ActiveSync.

Vous pouvez protéger ce répertoire virtuel de deux manières :

- **Protection de l'ensemble du serveur Web (conseillé)** Avec cette option, vous protégez toutes les racines virtuelles du serveur IIS comportant le composant RSA ACE/Agent, y compris les autres serveurs implémentés par le serveur frontal. Par exemple, vous pouvez avoir configuré votre serveur Exchange frontal comme point d'accès pour Outlook Mobile Access ou pour Outlook Web Access.
- **Protection des répertoires virtuels ActiveSync Exchange uniquement** Avec cette option, vous configurez le composant RSA ACE/Agent de sorte que SecurID protège uniquement ActiveSync Exchange. Utilisez cette option si vous avez l'intention d'activer des services supplémentaires, tels

qu'Outlook Web Access et Outlook Mobile Access, sur le même serveur sans protéger ces services à l'aide de SecurID.

Par défaut, le composant ACE/Agent est configuré pour protéger l'ensemble du serveur Web. Vous pouvez utiliser la procédure suivante pour vérifier cette configuration.

Pour vérifier que le composant ACE / Agent est configuré pour protéger l'ensemble du serveur Web

1. Dans le composant logiciel enfichable IIS pour MMC, cliquez avec le bouton droit sur le serveur Web par défaut et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet **RSA SecurID** et vérifiez que la case à cocher **Protect This Resource** est activée.

Utilisez la procédure suivante pour configurer le serveur frontal de manière à ce que l'authentification RSA SecurID soit limitée à ActiveSync Exchange.

Pour limiter l'authentification SecurID au répertoire virtuel ActiveSync Microsoft Exchange

1. Pour désactiver la protection à l'échelle du serveur, dans le composant logiciel enfichable IIS, cliquez avec le bouton droit sur le serveur Web par défaut puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **RSA SecurID** et désactivez la case à cocher **Protect This Resource**. (Cette opération permet de faire en sorte que RSA SecurID ne soit pas activé pour l'ensemble du serveur mais uniquement pour les racines virtuelles que vous spécifiez.)
3. Pour activer la protection des répertoires virtuels, dans le composant logiciel enfichable IIS, cliquez avec le bouton droit sur le répertoire virtuel ActiveSync Microsoft Server, puis cliquez sur **Propriétés**.
4. Sélectionnez l'onglet **RSA SecurID** et activez la case à cocher **Protect This Resource**.

   Remarque Si la case à cocher est activée et grisée, cela signifie que le répertoire virtuel hérite son paramètre du répertoire parent. Consultez les propriétés du répertoire parent et désactivez la case à cocher **Protect This Resource** si vous ne voulez pas que le répertoire parent soit protégé. Revenez ensuite sur le répertoire enfant et assurez-vous que la case à cocher est activée.

Personnalisation des en-têtes de réponse HTTP pour les périphériques

Le client ActiveSync du périphérique Microsoft Windows Mobile doit être en mesure de faire la distinction entre l'authentification RSA SecurID et les réponses ActiveSync Exchange. Pour cela, vous devez configurer des en-têtes de réponse HTTP personnalisés sur le répertoire virtuel WebID qui contient les formulaires HTML configurés par le composant RSA ACE/Agent.

Pour configurer des réponses HTTP personnalisés pour les périphériques

1. Dans le composant logiciel enfichable IIS pour MMC, recherchez le répertoire virtuel WebID sur le serveur frontal. Ce répertoire virtuel est créé par SecurID et contient les formulaires d'authentification et les réponses de SecurID.
2. Cliquez avec le bouton droit sur le répertoire virtuel WebID puis sur **Propriétés** afin d'ouvrir les propriétés de ce répertoire virtuel.
3. Cliquez sur l'onglet **En-tête HTTP,** cliquez sur le bouton **Ajouter**, puis entrez l'en-tête suivant :

   Remarque Veillez à respecter la casse et à saisir la valeur sur une seule ligne.

   ```
   Custom Header Name: MSAS-TwoFactorAuth Custom Header Value: True Custom Header Name: MS-ASProtocolVersions Custom Header Value: 1.0,2.0 Custom Header Name: MS-ASProtocolCommands Custom Header Value: Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,CreateCollection,DeleteCollection,MoveCollection,FolderSync,FolderCreate,FolderDelete,FolderUpdate,MoveItems,GetItemEstimate,MeetingResponse
   ```

Configuration de comptes d'utilisateur

Les comptes d'utilisateur pour SecurID doivent être configurés par l'Administrateur conformément aux recommandations de la documentation produit RSA SecurID, avec la restriction suivante :

- Pour tous les utilisateurs, les ID utilisateur SecurID sélectionnés doivent correspondre à leur nom de compte Windows. ActiveSync Exchange avec SecurID ne fonctionne pas pour les utilisateurs possédant une ID RSA distincte, qui ne correspond pas à leur nom de compte Windows.

Configuration d'Outlook Mobile Access

Par défaut, tous les utilisateurs sont activés pour Exchange ActiveSync et Outlook Mobile Access. Cependant, seul ActiveSync Exchange est activé sur le serveur Exchange ; par défaut, Outlook Mobile Access est désactivé. Cette section décrit comment activer Outlook Mobile Access sur votre serveur Exchange.

Pour permettre à vos utilisateurs Exchange 2003 d'utiliser Outlook Mobile Access, procédez comme suit :

1. Configurez votre serveur frontal Exchange 2003 pour Outlook Mobile Access.
2. Activez Outlook Mobile Access sur le serveur Exchange.
3. Configurez les périphériques utilisateur pour qu'ils utilisent une connexion mobile.
4. Apprenez à vos utilisateurs comment utiliser Outlook Mobile Access.

Configuration du serveur frontal Exchange 2003 pour Outlook Mobile Access

Par défaut, le répertoire virtuel Outlook Mobile Access (qui permet à vos utilisateurs d'accéder à Exchange à partir d'un périphérique mobile) est installé avec Exchange 2003. Ce répertoire virtuel possède les mêmes paramètres de configuration que le répertoire virtuel Outlook Web Access. Lorsque vous configurez un serveur pour qu'il utilise Outlook Mobile Access, vous devez suivre la même procédure que pour configurer un serveur pour Outlook Web Access. Pour plus d'informations sur la configuration de vos serveurs Exchange 2003 pour qu'ils utilisent Outlook Web Access, consultez le guide (en anglais) *Using Microsoft Exchange 2000 Front-End Servers* (http://go.microsoft.com/fwlink/?linkid=12055).

Activation d'Outlook Mobile Access sur le serveur Exchange

Après avoir configuré votre serveur frontal pour qu'il utilise Outlook Mobile Access, vous devez activer Outlook Mobile Access sur vos serveurs Exchange.

Pour activer Outlook Mobile Access pour votre organisation

1. Ouvrez la session comme Administrateur Exchange sur le serveur Exchange sur lequel se trouve la boîte aux lettres de l'utilisateur et démarrez le Gestionnaire système Exchange.
2. Développez **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. À la page **Propriétés des services mobiles**, dans **Outlook Mobile Access**, sélectionnez **Activer Outlook Mobile Access**.
4. Pour permettre aux utilisateurs d'utiliser des périphériques qui ne sont pas pris en charge, activez la case à cocher **Activer les périphériques non pris en charge**.

   Remarque Pour plus d'informations sur les périphériques pris en charge pour Exchange et la planification de la prise en charge de périphériques mobiles avec Exchange, consultez le guide *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766).
5. Cliquez sur **OK**.

Après avoir activé Outlook Mobile Access, vous pouvez modifier les paramètres Outlook Mobile Access pour les utilisateurs ou les groupes d'utilisateurs à l'aide du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.

Configuration des périphériques utilisateur pour qu'ils utilisent une connexion mobile

Pour accéder à Exchange 2003 à l'aide d'Outlook Mobile Access, vos utilisateurs doivent posséder un périphérique mobile provenant d'un opérateur mobile qui dispose d'un réseau informatique établi pour les données mobiles. Avant que vos utilisateurs se connectent à Exchange 2003 et utilisent Outlook Mobile Access ou ActiveSync Exchange via une connexion mobile, vous devez leur apprendre à configurer leurs périphériques pour utiliser un réseau mobile, ou au moins leur indiquer les ressources à leur disposition pour cet apprentissage. Pour plus d'informations sur la configuration des périphériques mobiles et ActiveSync Exchange, consultez la section « Pour configurer les périphériques Pocket PC Phone Edition afin qu'ils utilisent ActiveSync Exchange », plus haut dans ce chapitre.

Formation de vos utilisateurs à l'utilisation d'Outlook Mobile Access

Après avoir configuré Exchange 2003 pour Outlook Mobile Access et une fois que vos utilisateurs possèdent des périphériques mobiles capables d'utiliser un réseau mobile pour accéder aux serveurs Exchange 2003, vos utilisateurs ont besoin de savoir comment accéder à leur serveur Exchange et utiliser Outlook Mobile Access. La procédure ci-dessous permet d'utiliser Outlook Mobile Access sur un périphérique Pocket PC Phone Edition.

Pour configurer un périphérique Pocket PC Phone Edition pour qu'il utilise Outlook Mobile Access

1. Sur le périphérique, sur l'écran Aujourd'hui, appuyez sur **Démarrer** puis sur **Internet Explorer**.
2. Sur l'écran **Internet Explorer**, tapez sur **Affichage**, puis sur **Barre d'adresses** pour afficher la barre d'adresses dans la fenêtre du navigateur.
3. Tapez n'importe où dans la barre d'adresses, entrez l'URL suivante, puis tapez sur le bouton **OK** : https://*NomServeurExchange*/oma**,** où *NomServeurExchange* correspond au nom du serveur Exchange qui exécute Outlook Mobile Access.

   Remarque Si une bulle de connexion ne s'affiche pas, vous devrez peut-être vous connecter manuellement à votre réseau.
4. Sur l'écran **Ouverture de session sur le réseau**, entrez le nom d'utilisateur, mot de passe et domaine dans les espaces fournis, puis cliquez sur **OK**.
5. Répétez cette procédure pour chacun des périphériques Pocket PC Phone Edition de vos utilisateurs. Au lieu de cela, vous pouvez apprendre à vos utilisateurs à configurer eux-mêmes leurs périphériques en vue d'une utilisation avec ActiveSync Exchange.

Configuration d'Outlook Web Access

Par défaut, Outlook Web Access est activé pour l'ensemble des utilisateurs après l'installation d'Exchange 2003. Toutefois, vous pouvez activer les fonctionnalités suivantes pour Outlook Web Access :

- Configuration d'une page d'ouverture de session
- Configuration de l'authentification
- Configuration des options de sécurité
- Configuration de la compression Outlook Web Access
- Simplification de l'URL d'Outlook Web Access

Configuration d'une page d'ouverture de session

Vous pouvez activer une nouvelle page d'ouverture de session Outlook Web Access qui enregistre le nom et le mot de passe de l'utilisateur dans un cookie plutôt que dans le navigateur. Lorsque l'utilisateur ferme son

navigateur, le cookie est supprimé. De plus, après un certain temps d'inactivité, le cookie est supprimé automatiquement. La nouvelle page d'ouverture de session nécessite que l'utilisateur entre soit son nom de domaine, nom d'utilisateur et son mot de passe soit son adresse de messagerie UPN (User Principal Name) complète et son mot de passe, pour accéder à la messagerie.

Pour activer cette page d'ouverture de session, vous devez d'abord activer l'authentification par formulaires sur le serveur, puis sécuriser la page d'ouverture de session en définissant le délai d'expiration du cookie et en adaptant les paramètres de sécurité côté client.

Activation de l'authentification basée sur les formulaires

Pour activer la page d'ouverture de session Outlook Web Access, vous devez activer l'authentification par formulaires sur le serveur.

Pour activer l'authentification par formulaires

1. Sur le serveur Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez le Gestionnaire système Exchange.
2. Dans l'arborescence de la console, développez **Serveurs**.
3. Développez le serveur pour lequel vous souhaitez activer l'authentification par formulaires, puis développez **Protocoles**.
4. Développez **HTTP,** cliquez avec le bouton droit sur **Serveur virtuel Exchange**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés du serveur virtuel Exchange**, sous l'onglet **Paramètres** du volet Outlook Web Access, activez l'option **Activer l'authentification basée sur les formulaires**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Définition du délai d'expiration de l'authentification des cookies

Dans Exchange 2003, les informations d'identification des utilisateurs Outlook Web Access sont stockées dans un cookie. Lorsque l'utilisateur ferme la session Outlook Web Access, le cookie est supprimé et n'est plus valide pour l'authentification. Par ailleurs, par défaut, si votre utilisateur utilise un ordinateur public et sélectionne l'option **Ordinateur public ou partagé** de l'écran d'ouverture de session d'Outlook Web Access, le cookie sur cet ordinateur expire automatiquement après 15 minutes d'inactivité de l'utilisateur.

Le délai d'expiration automatique est utile car il permet de protéger le compte d'un utilisateur contre les accès non autorisés. Toutefois, bien que le délai d'expiration automatique réduise les risques d'accès non autorisé, il n'élimine pas complètement la possibilité qu'un utilisateur non autorisé accède à un compte Outlook Web Access si une session continue à s'exécuter sur un ordinateur public. Par conséquent, veillez à ce que vos utilisateurs connaissent les précautions à prendre pour éviter ces risques.

Pour répondre aux besoins de sécurité de votre organisation, un administrateur peut configurer les délais d'expiration après inactivité sur le serveur frontal Exchange. Pour modifier cette valeur, vous devez modifier les paramètres du Registre sur le serveur.

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données utiles.

Pour spécifier le délai d'expiration du cookie d'authentification par formulaires Outlook Web Access de l'ordinateur public

1. Sur le serveur frontal Exchange, ouvrez une session avec le compte d'administrateur Exchange et démarrez l'Éditeur du Registre (**regedit**).

2. Dans l'Éditeur du Registre, recherchez la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   MSExchangeWeb\OWA
   ```

3. Dans le menu **Edition**, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.
4. Dans le volet d'informations, nommez la nouvelle valeur **PublicClientTimeout**.
5. Cliquez avec le bouton droit sur la valeur DWORD **PublicClientTimeout**, puis cliquez sur **Modifier**.
6. Dans **Édition de la valeur DWORD**, sous **Base**, cliquez sur **Décimale**.
7. Dans la zone **Données de la valeur**, tapez une valeur (en minutes) comprise entre 1 et 432,000.
8. Cliquez sur **OK**.

Configuration des options de sécurité de client pour les utilisateurs

La page d'ouverture de session Outlook Web Access permet à l'utilisateur de sélectionner l'option de sécurité qui répond le mieux à ses besoins. L'option **Ordinateur public ou partagé** (sélectionnée par défaut) prend en charge un court délai d'expiration par défaut de 15 minutes. Un utilisateur doit sélectionner l'option **Ordinateur privé**, seulement s'il est le seul à travailler sur l'ordinateur et si cet ordinateur participe aux stratégies de sécurité mises en place dans l'organisation de cet utilisateur. Lorsqu'elle est activée, l'option **Ordinateur privé** accepte une période d'inactivité beaucoup plus longue avant de clore automatiquement la session. La valeur interne par défaut est de 24 heures. Fondamentalement, cette option est destinée aux utilisateurs Outlook Web Access, qui utilisent des ordinateurs personnels à leur bureau ou à domicile.

Pour respecter les besoins de sécurité de votre organisation, un administrateur peut configurer des délais d'expiration après inactivité.

> **Remarque** La valeur par défaut du délai d'expiration du cookie de l'ordinateur public est de quinze minutes. Pour modifier cette valeur, vous devez modifier les paramètres du Registre sur le serveur.
>
> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données utiles.

Pour spécifier le délai d'expiration du cookie public d'authentification par formulaires Outlook Web Access

1. Démarrez l'Éditeur du Registre (**regedit**).
2. Naviguez jusqu'à la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
   Services\MSExchangeWeb\OWA
   ```

3. Dans le menu **Edition**, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.
4. Dans le volet d'informations, nommez la nouvelle valeur **PublicClientTimeout**.
5. Cliquez avec le bouton droit sur la valeur Dword **PublicClientTimeout**, puis cliquez sur **Modifier**.
6. Dans **Édition de la valeur DWORD**, sous **Base**, cliquez sur **Décimale**.
7. Dans la zone **Données de la valeur**, tapez une valeur (en minutes) comprise entre 1 et 432,000.
8. Cliquez sur **OK**.

Pour spécifier le délai d'expiration du cookie client approuvé d'authentification par formulaires Outlook Web Access

1. Démarrez l'Éditeur du Registre (**regedit**).
2. Naviguez jusqu'à la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
   Services\MSExchangeWeb\OWA
   ```

3. Dans le menu **Edition**, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.

4. Dans le volet d'informations, nommez la nouvelle valeur **TrustedClientTimeout**.
5. Cliquez avec le bouton droit sur la valeur Dword **TrustedClientTimeout**, puis cliquez sur **Modifier**.
6. Dans **Édition de la valeur DWORD**, sous **Base**, cliquez sur **Décimale**.
7. Dans la zone **Données de la valeur**, tapez une valeur (en minutes) comprise entre 1 et 432,000.
8. Cliquez sur **OK**.

Compression Outlook Web Access

Outlook Web Access prend en charge la compression des données, ce qui est optimal pour les connexions réseau lentes. Selon le paramètre de compression utilisé, la compression Outlook Web Access permet de compresser des pages Web statiques, des pages Web dynamiques, ou les deux. Le tableau 2.1 répertorie les paramètres de compression disponibles dans Exchange Server 2003 pour Outlook Web Access.

Tableau 2.1 Paramètres de compression disponibles pour Outlook Web Access

Paramètre de compression	Description
Haut	Compression des pages statiques et des pages dynamiques.
Bas	Compression des pages statiques uniquement.
Aucun	Aucune compression n'est effectuée.

Conditions requises pour la compression Outlook Web Access

Pour utiliser la compression des données pour Outlook Web Access dans Exchange Server 2003, vous devez vérifier que votre organisation remplit les conditions requises suivantes :

- Le serveur Exchange auprès duquel les utilisateurs s'authentifient pour Outlook Web Access doit exécuter Windows Server 2003.
- Les boîtes aux lettres de vos utilisateurs doivent se trouver sur des serveurs Exchange 2003. (Si vous disposez d'un déploiement mixte de boîtes aux lettres Exchange, vous pouvez créer un serveur virtuel supplémentaire sur votre serveur Exchange, destiné uniquement aux utilisateurs Exchange 2003, et activer la compression sur ce serveur.)
- Les ordinateurs clients doivent exécuter Internet Explorer version 6 ou ultérieure. Les ordinateurs clients doivent également exécuter Windows XP ou Windows 2000 et comporter la mise à jour de sécurité décrite dans le bulletin MS02-066, « Correctif cumulatif pour Internet Explorer (Q328970) » (http://go.microsoft.com/fwlink/?LinkId=16694).

  Remarque Si un utilisateur ne possède pas de navigateur prenant en charge la compression, l'ordinateur client continue à se comporter normalement.
- Vous devrez peut-être activer la prise en charge de HTTP 1.1 par le biais de serveurs Proxy pour certaines connexions d'accès à distance. (La prise en charge de HTTP 1.1 est requise pour que la compression fonctionne correctement.)

Pour activer la compression des données Outlook Web Access

1. Démarrez le Gestionnaire système Exchange.
2. Dans le volet d'informations, développez **Serveurs**, développez le serveur de votre choix, puis développez **Protocoles**.
3. Développez **HTTP,** cliquez avec le bouton droit sur **Serveur virtuel Exchange**, puis cliquez sur **Propriétés**.

4. Dans **Propriétés du serveur virtuel Exchange**, dans l'onglet **Paramètres**, sous **Outlook Web Access**, utilisez la liste **Compression** pour sélectionner le niveau de compression que vous voulez (**Aucun**, **Bas** ou **Haut**).
5. Cliquez sur **Appliquer**, puis sur **OK**.

Simplification de l'URL d'Outlook Web Access

Le serveur virtuel HTTP qui est créé par Exchange pendant l'installation met à disposition les URL suivantes pour l'accès des utilisateurs :

- **http://*nom_serveur*/public** Cette URL donne accès aux dossiers publics.
- **http://*nom_serveur*/exchange/*nom_boîte_aux_lettres*** Cette URL donne accès aux boîtes aux lettres.

Les utilisateurs demandent fréquemment qu'une URL plus simple que l'URL par défaut soit mise à leur disposition pour l'accès à leurs boîtes aux lettres. Cette URL simplifiée facilite à la fois la mémorisation et la saisie de l'URL dans un navigateur Web. Par exemple, http://www.contoso1.com est une URL plus facile à mémoriser pour les utilisateurs que http://contosoexchange01/exchange.

La procédure suivante permet de simplifier l'URL utilisée pour accéder à Outlook Web Access. Elle configure une demande, envoyée au répertoire racine du serveur Web (http://*nom_serveur*/), de redirection vers le répertoire virtuel Exchange. Par exemple, une demande à http://*nom_serveur*/ est dirigée vers http://*nom_serveur*/exchange/, qui déclenche ensuite une ouverture de session implicite.

Pour simplifier l'URL d'Outlook Web Access

1. À l'aide du Gestionnaire des services Internet, ouvrez les propriétés du site Web par défaut.
2. Cliquez sur l'onglet **Répertoire de base**, puis sélectionnez **Une redirection vers une URL**.
3. Dans **Rediriger vers**, tapez /*nom répertoire*, puis cliquez sur **Un répertoire situé sous l'adresse URL entrée**.

   Par exemple, pour rediriger les demandes http://mail/ vers http://mail/exchange, dans **Rediriger vers**, tapez /exchange.
4. Pour demander aux utilisateurs d'utiliser SSL (Secure Sockets Layer), dans **Rediriger vers**, tapez https://mail/*nom répertoire*, puis cliquez sur l'option **L'URL exacte entrée ci-dessus**.

   Ce paramètre pré-programme le nom du serveur. Si, par conséquent, vous redirigez les demandes des clients vers https://mail, le client doit pouvoir résoudre le nom « mail ».

Pour plus d'informations sur une autre méthode de redirection des clients vers SSL, consultez l'article 279681 de la Base de connaissances Microsoft, « How to Force SSL Encryption for an Outlook Web Access 2000 Client » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=279681).

Configuration des serveurs virtuels POP3 et IMAP4

Par défaut, sur une nouvelle installation Exchange Server 2003, les serveurs virtuels POP3 et IMAP4 sont désactivés. Pour les activer, vous devez commencer par utiliser le composant enfichable Services de MMC et définir les services pour qu'ils démarrent automatiquement. Si vous configurez les services pour un démarrage automatique et avez par la suite besoin de les démarrer, de les suspendre ou de les arrêter, utilisez le Gestionnaire système Exchange.

Pour démarrer, suspendre et arrêter le serveur virtuel

1. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur le serveur virtuel IMAP4 ou POP3.
2. Sélectionnez l'une des options suivantes :
   - **Démarrer** Démarre le serveur virtuel.

- **Suspendre** Fait passer l'état du serveur sur Suspendu ; une icône apparaît en regard du nom du serveur dans l'arborescence de la console. Pour redémarrer le serveur, cliquez de nouveau sur **Suspendre**.
- **Arrêter** Fait passer l'état du serveur sur Arrêté ; une icône apparaît en regard du nom du serveur dans l'arborescence de la console.

Gestion de l'accès client à Exchange Server 2003

Ce chapitre décrit la gestion des paramètres d'accès client pour les protocoles et les clients que vous prenez en charge. Ce chapitre passe également en revue les concepts fondamentaux de l'accès client, indique comment gérer les protocoles utilisés par les clients qui accèdent à Microsoft® Exchange Server 2003 et décrit l'architecture serveur frontal/principal.

> **Remarque** Pour gérer correctement l'accès client à Exchange 2003, vous devez bien comprendre comment les technologies Microsoft Windows®, telles que les services Internet et le service d'annuaire Microsoft Active Directory®, interagissent avec Exchange. Vous devez également être familiarisé avec les protocoles, tels que HTTP et MAPI, et comprendre comment les applications clientes comme ActiveSync® Exchange et Microsoft Office Outlook® 2003 utilisent respectivement ces protocoles pour interagir avec Exchange.

Gestion des protocoles

Dans votre configuration de déploiement de la messagerie Exchange, utilisez le Gestionnaire système Exchange pour gérer les protocoles que vous prenez en charge. Lorsque vous utilisez le Gestionnaire système Exchange pour gérer des protocoles, vous manipulez des paramètres sur les serveurs virtuels associés au protocole qui doit être configuré. Les serveurs virtuels associés aux divers protocoles, tels que le serveur virtuel Exchange et le serveur virtuel IMAP4 (Internet Message Access Protocol version 4rev1), contiennent des paramètres fondés sur les capacités et sur l'utilisation du protocole considéré. Ainsi, le serveur virtuel Exchange, qui gère l'accès HTTP à Exchange, fournit les paramètres associés à Microsoft Office Outlook 2003 Web Access comme la prise en charge de la compression gzip.

En principe, la gestion du serveur virtuel pour un protocole déterminé est similaire à la gestion d'un serveur virtuel pour un autre protocole. Les tâches communes de gestion sont l'activation d'un serveur virtuel, l'affectation de ports, la définition des limites de connexion, le démarrage et l'arrêt d'un serveur virtuel et la déconnexion des utilisateurs. Il existe cependant des tâches de gestion spécifiques aux serveurs. Les sections suivantes décrivent les tâches communes à tous les serveurs virtuels qui se rapportent aux protocoles, ainsi que les tâches spécifiques au serveur virtuel Exchange, au serveur virtuel IMAP4 et au serveur virtuel NNTP (Network News Transfer Protocol).

> **Remarque** Pour gérer les paramètres individuels d'accès client à Exchange, utilisez Utilisateurs et ordinateurs Active Directory.

Activation d'un serveur virtuel

Lorsque vous installez Exchange, les services nécessaires à la prise en charge des clients comme Outlook 2003, Outlook Web Access et Exchange ActiveSync sont activés par défaut. Par exemple, Exchange active le service SMTP parce que c'est le protocole sous-jacent utilisé pour acheminer les messages à la fois en interne au sein d'une organisation Exchange et en externe vers les systèmes de messagerie situés à l'extérieur d'une organisation Exchange. De la même façon, Exchange active HTTP car c'est le protocole sous-jacent pour toutes les communications Internet.

> **Remarque** **Bien** qu'il utilise le protocole HTTP, Outlook Mobile Access est désactivé par défaut et doit être activé à l'aide du Gestionnaire système Exchange.

Cependant, Exchange installe, mais n'active pas de services pour POP3 (Post Office Protocol version 3), IMAP4 et NNTP. Si votre modèle d'accès client repose sur des communications qui utilisent POP3, IMAP4 ou NTTP, vous devez les activer manuellement.

Pour activer le service POP3 ou IMAP4, utilisez le composant logiciel enfichable Services pour instaurer un démarrage automatique du service. Démarrez ensuite le service à l'aide du Gestionnaire système Exchange. Pour activer NNTP, définissez, à l'aide du composant logiciel enfichable Services, un démarrage automatique du service NNTP (Network News Transfer Protocol service ou NntpSVC), puis démarrez le service à l'aide du Gestionnaire système Exchange.

Pour activer le démarrage automatique du serveur virtuel POP3 ou IMAP4

1. Dans le composant logiciel enfichable **Services**, dans l'arborescence de la console, cliquez sur **Services (local)**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Microsoft Exchange POP3** ou sur **Microsoft Exchange IMAP4**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, sous **Type de démarrage**, sélectionnez **Automatique**, puis cliquez sur **Appliquer**.
4. Sous **État du service**, cliquez sur **Démarrer**, puis sur **OK**.
5. Répétez cette procédure sur tous les nœuds qui doivent héberger le serveur virtuel POP3 ou IMAP4.

Pour activer un serveur virtuel NNTP

1. Dans le composant logiciel enfichable **Services**, dans l'arborescence de la console, cliquez sur **Services (local)**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Network News Transport Protocol (NNTP)**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, sous **Type de démarrage**, sélectionnez **Automatique**, puis cliquez sur **OK**.

Pour démarrer un serveur virtuel POP3, IMAP4 ou NTTP

1. Dans le Gestionnaire système Exchange, développez **Protocoles**, développez le protocole approprié (**POP3**, **IMAP4** ou **NNTP**), cliquez avec le bouton droit sur le serveur virtuel par défaut approprié (**Serveur virtuel POP3 par défaut**, **Serveur virtuel IMAP par défaut** ou **Serveur virtuel NNTP par défaut**), puis cliquez sur **Démarrer**.

Affectation de ports et d'une adresse IP à un serveur virtuel

Lorsque vous créez un serveur virtuel pour un protocole, vous avez la possibilité d'utiliser les affectations de port par défaut ainsi que l'adresse IP (Internet Protocol) du serveur. Le tableau 3.1 indique les affectations de port par défaut associées aux protocoles. L'adresse IP par défaut est **(Non assignée)**, ce qui signifie qu'aucune adresse IP déterminée n'a été affectée et que le serveur virtuel utilisera l'adresse IP du serveur Exchange qui héberge le serveur virtuel. Ces valeurs par défaut dotent un serveur virtuel des capacités de détection automatique (le serveur reçoit immédiatement les connexions entrantes à l'aide de l'adresse IP et des ports par défaut).

Tableau 3.1 Affectations de port par défaut

Protocoles	Port TCP	Port SSL (Secure Sockets Layer)
SMTP	25	Non disponible
IMAP4	143	993
POP3	110	995
NNTP	119	563

Important Si vous n'utilisez pas les affectations de port recommandées, il est possible que certains clients ne puissent pas se connecter. Vous pouvez également avoir à reconfigurer manuellement le logiciel client pour établir la connexion avec les nouvelles affectations de ports.

Remarque Pour activer intégralement SSL sur le serveur virtuel POP3, vous devez demander et installer un certificat. Cette opération est nécessaire même si le port SSL par défaut est défini sur 995 sur le serveur virtuel POP3. Pour plus d'informations sur l'installation de certificats, consultez « *Sécurisation des communications » et « Configuration de Microsoft Exchange Server 2003 pour l'accès client », du Guide de déploiement d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

L'utilisation des affectations de port par défaut est fortement recommandée, mais celle de l'adresse IP par défaut n'est pas imposée. Vous pouvez utiliser l'adresse IP de n'importe quelle carte réseau disponible en tant qu'adresse IP du serveur virtuel.

Si vous envisagez de créer plusieurs serveurs virtuels, chacun d'eux doit avoir une combinaison unique de ports et d'adresse IP. Comme la configuration des ports est standard et ne doit pas être modifiée, vous devez fournir une adresse IP unique à chaque serveur virtuel.

Outre une combinaison unique de ports et d'adresse IP pour chaque serveur virtuel, vous pouvez également configurer plusieurs identités. La pluralité des identités vous permet d'associer plusieurs noms d'hôte ou de domaine à un seul serveur virtuel.

La procédure suivante permet d'affecter une adresse IP unique à un serveur virtuel ou d'affecter plusieurs identités à un serveur virtuel.

Pour affecter une adresse IP ou une identité à un serveur virtuel

1. Connectez-vous au serveur Exchange sur lequel le serveur virtuel s'exécute, ouvrez une session avec un compte d'administrateur Exchange doté d'autorisations d'administration locales et d'autorisations d'administration intégrales Exchange.
2. Dans le Gestionnaire système Exchange, développez **Protocoles**, cliquez avec le bouton droit sur le protocole auquel doit être affectée une nouvelle adresse IP ou auquel vous souhaitez ajouter une nouvelle identité, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, cliquez sur **Paramètres avancés**.
4. Dans la boîte de dialogue **Paramètres avancés**, cliquez sur **Modifier** pour attribuer à l'adresse IP une valeur unique, ou cliquez sur **Ajouter** pour ajouter une nouvelle identité (c'est-à-dire une nouvelle combinaison d'adresse IP et de ports).

Définition de limites de connexion

Le nombre de connexions entrantes que peut accepter un serveur virtuel est uniquement limité par les ressources de l'ordinateur qui héberge ce serveur. Pour éviter de surcharger un ordinateur, vous pouvez limiter le nombre de connexions simultanées réalisables vers le serveur virtuel. Par défaut, Exchange n'impose aucune limite au nombre de connexions entrantes.

Dès que les utilisateurs sont connectés, vous pouvez aussi définir le délai au-delà duquel les connexions inactives sont déconnectées du serveur. Par défaut, Exchange déconnecte les sessions inactives après 10 minutes.

Dans les topologies comportant des serveurs Exchange frontaux et principaux, le paramétrage du délai de connexion varie selon le rôle du serveur. Sur les serveurs principaux, le délai de connexion limite le temps pendant lequel les clients peuvent rester connectés au serveur sans activité. Sur les serveurs frontaux, cette valeur définit la durée totale maximale de la session cliente quelle que soit l'activité du client. Par conséquent, dans les environnements frontaux/principaux, vous devez définir un délai suffisamment élevé sur vos serveurs frontaux pour que vos utilisateurs puissent télécharger un message de la taille maximale autorisée avec la vitesse de connexion la plus lente prise en charge. Une valeur suffisamment élevée garantit que les clients ne seront pas déconnectés pendant qu'ils téléchargent des messages. Pour plus d'informations sur la configuration d'une architecture serveur frontal/principal Exchange, consultez le Guide de déploiement d'*Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

Avertissement Si le délai de connexion défini est trop court, les clients peuvent être déconnectés du serveur de façon inattendue et recevoir des messages d'erreur. Le délai de déconnexion minimal recommandé est de trente minutes.

Pour définir des limites de connexion

1. Connectez-vous au serveur Exchange sur lequel le serveur virtuel s'exécute, ouvrez une session avec un compte d'administrateur Exchange doté d'autorisations d'administration locales et d'autorisations d'administration intégrales Exchange.
2. Dans le Gestionnaire système Exchange, développez **Protocoles**, cliquez avec le bouton droit sur le protocole pour lequel vous souhaitez modifier les limites de connexion, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, définissez les limites de connexion appropriées.

Démarrage, mise en suspens ou arrêt d'un serveur virtuel

La gestion de serveurs virtuels requiert fréquemment de démarrer, de mettre en suspens ou d'arrêter les services Exchange. La gestion des services Exchange s'effectue par le biais de la console Gestion de l'ordinateur et du Gestionnaire système Exchange.

Pour démarrer, suspendre ou arrêter un serveur virtuel

1. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur le serveur virtuel que vous souhaitez gérer, puis effectuez l'une des opérations suivantes :
2. Pour démarrer le service, cliquez sur **Démarrer**.
3. Pour modifier l'état du serveur suspendu ou pour redémarrer un serveur suspendu, cliquez sur **Suspendre**.

   Remarque Lorsqu'un serveur est suspendu, une icône correspondante apparaît en regard de son nom dans l'arborescence de la console.
4. Pour changer l'état du serveur à arrêter, cliquez sur **Arrêter**.

   Remarque Lorsqu'un serveur est arrêté, une icône correspondante apparaît en regard de son nom dans l'arborescence de la console.

Déconnexion des utilisateurs

Vous pouvez instantanément déconnecter un utilisateur déterminé ou tous les utilisateurs en cas d'accès non autorisé au serveur virtuel.

Pour déconnecter tous les utilisateurs

1. Dans le Gestionnaire système Exchange, développez **SMTP**, **IMAP4** ou **POP3**, puis double-cliquez sur le serveur virtuel sur lequel vous souhaitez déconnecter les utilisateurs.
2. Pour déconnecter les utilisateurs, exécutez l'une des méthodes suivantes à partir du nœud **Sessions en cours** sous le serveur virtuel :
   - Pour déconnecter un utilisateur déterminé, cliquez sur **Fermer**.
   - Pour déconnecter tous les utilisateurs, cliquez sur **Fermer tout**.

Gestion des options de calendrier des serveurs virtuels POP3 et IMAP4

Vous avez la possibilité de configurer une URL qui donne un accès aux informations de calendrier à vos clients de messagerie POP3 et IMAP4. Cette fonctionnalité vous permet d'utiliser un client de messagerie POP3 ou IMAP4 et Outlook Web Access pour gérer votre calendrier. Les options que vous sélectionnez pour cette fonctionnalité gèrent le format de l'URL.

Remarque Dans les topologies comportant des serveurs frontaux et principaux Exchange, vous configurez l'URL utilisée pour accéder aux informations de calendrier sur le serveur principal. Exchange ne reconnaît aucun des paramètres d'URL que vous configurez sur les serveurs frontaux.

Lorsque les demandes de réunions sont téléchargées par le biais de POP3 et d'IMAP4, une URL liée à la demande de réunion Outlook Web Access est ajoutée à la partie en texte brut/HTML du message. Les utilisateurs cliquent sur l'URL pour accéder à la demande de réunion, puis acceptent ou refusent la demande (certains clients de messagerie IMAP4 et POP3 incluent une interface utilisateur graphique (GUI) qui leur permet d'accepter ou de décliner les réunions sans cliquer sur l'URL). Si les utilisateurs acceptent la demande, Exchange l'ajoute automatiquement à leur calendrier.

Remarque L'URL à la demande de réunion ne fonctionne pas pour les clients POP3 configurés pour télécharger des messages à partir du serveur. Cette situation se produit parce que le message est téléchargé sur le client. Il en résulte que l'URL pointe sur un message qui ne figure plus sur le serveur.

Pour configurer les options de calendrier pour un serveur virtuel POP3 ou IMAP4

1. Dans le Gestionnaire système Exchange, développez le **Premier groupe d'administration**, développez le nœud **Serveurs**, puis développez le serveur Exchange pour lequel vous souhaitez gérer les options de calendrier POP3 ou IMAP4.
2. Développez le nœud **Protocoles**, puis cliquez avec le bouton droit sur le protocole POP3 ou IMAP4, puis sélectionnez **Propriétés**.
3. Sous l'onglet **Calendrier**, sélectionnez le serveur d'où les destinataires téléchargent les demandes de réunion :
   - Pour désigner le serveur associé du destinataire en tant que serveur à partir duquel le destinataire téléchargera les demandes de réunion, sélectionnez **Utiliser le serveur du destinataire**.

     Il s'agit de l'option activée par défaut. Si vous sélectionnez cette option, l'URL adopte le format suivant :

     `http://<HomeServerName>/Exchange/Username/Inbox/Team%20Meeting.eml`
   - Pour désigner un serveur frontal en tant que serveur à partir duquel les destinataires téléchargeront les demandes de réunion, sélectionnez **Utiliser un serveur frontal**.

     Cette option est utile si vous avez configuré vos utilisateurs Outlook Web Access pour qu'ils accèdent à leurs boîtes aux lettres par le biais d'un serveur frontal. Si vous sélectionnez cette option, l'URL adopte le format suivant :

     `http://<FQDomainName>/Exchange/Username/Inbox/Team%20Meeting.eml`
4. Pour utiliser SSL pour la connexion aux serveurs Exchange, sélectionnez **Utiliser des connexions SSL**.

   Remarque Si vous sélectionnez cette option, la syntaxe de l'URL comprend https:// au lieu de http://.
5. Cliquez sur **OK** pour enregistrer vos paramètres.

Gestion du serveur virtuel HTTP

Outlook Web Access, Outlook Mobile Access et ActiveSync Exchange s'appuient sur le protocole HTTP pour accéder aux informations Exchange. Ces clients utilisent également le protocole WebDAV, un ensemble de règles permettant aux ordinateurs d'échanger des informations, d'exécuter des instructions par le biais du serveur frontal Exchange et de gérer des informations dans la banque Exchange. Dans la mesure où il prend en charge HTTP et WebDAV, Exchange 2003 peut fournir aux utilisateurs un accès à un plus grand nombre de données. Par exemple, les utilisateurs Outlook Web Access peuvent effectuer des opérations de demande de calendrier et stocker des fichiers Microsoft Office, comme des documents Microsoft Office Word, dans la banque Exchange.

Exchange assure la prise en charge de HTTP et de WebDAV par le biais du serveur virtuel HTTP. Lorsque vous installez Exchange, Exchange installe et configure automatiquement un serveur virtuel HTTP. L'administration de ce serveur par défaut s'effectue uniquement à partir des services Internet (IIS).

Cependant, pour assurer différents scénarios de collaboration et pour accroître l'accès aux dossiers fournis par défaut par le site Web des services Internet, vous pouvez créer de nouveaux serveurs virtuels HTTP dans le Gestionnaire système Exchange. Comme n'importe quel serveur virtuel, chaque nouveau serveur virtuel HTTP que vous créez requiert une combinaison unique d'adresse IP, de port TCP, de port SSL et de nom d'hôte. Par

ailleurs, pour chaque serveur virtuel créé, vous devez définir un répertoire virtuel en tant que répertoire racine du serveur pour la publication du contenu.

> **Remarque** Le contenu de dossiers qui est affiché par le serveur virtuel HTTP est converti en pages Web et envoyé au navigateur d'un utilisateur par les services Internet (IIS).

Pour créer un nouveau serveur virtuel HTTP

1. Dans le Gestionnaire système Exchange, développez le **Premier groupe d'administration**, développez le nœud **Serveurs**, puis développez le serveur Exchange sur lequel vous souhaitez créer un nouveau répertoire virtuel HTTP.
2. Développez le nœud **Protocoles**, cliquez avec le bouton droit sur le protocole HTTP, sélectionnez **Nouveau**, puis cliquez sur **Serveur virtuel HTTP**.
3. Dans la boîte de dialogue **Propriétés** du nouveau serveur virtuel HTTP, configurez les paramètres du nouveau répertoire virtuel Exchange.

Gestion du serveur virtuel Exchange

Le serveur virtuel Exchange contient les répertoires virtuels offrant un accès à Exchange aux clients HTTP pris en charge par Exchange (par exemple, Outlook Web Access, Outlook Mobile Access et ActiveSync Exchange). Vous activez les paramètres d'Outlook Web Access, y compris l'authentification par formulaires et la compression gzip, à l'aide du serveur virtuel Exchange, mais vous gérez la plupart des paramètres des répertoires virtuels Exchange dans le composant logiciel enfichable IIS.

Plus particulièrement, dans Exchange 2003, si vous devez configurer les paramètres d'authentification de vos répertoires virtuels Exchange, utilisez le composant logiciel enfichable IIS. Pour configurer le contrôle d'accès aux répertoires virtuels \Exchange, \Public et \Exadmin, utilisez plutôt le Gestionnaire système Exchange.

Utilisation des paramètres IMAP4

Le serveur virtuel IMAP4 a deux paramètres spécifiques au protocole :

- **Inclure tous les dossiers publics quand la liste est demandée** Contrairement à POP3, qui donne aux clients un accès uniquement aux messages électroniques, IMAP4 permet aux clients d'accéder à d'autres dossiers en plus du dossier Boîte de réception. Cette possibilité d'accès aux autres dossiers doit toutefois être activée sur le serveur virtuel.
- **Activer la récupération rapide des messages** La récupération rapide des messages opère plus rapidement, car la taille des messages est évaluée approximativement et non pas calculée précisément. Le traitement est plus rapide, car le processeur est moins sollicité.

Vous sélectionnez ces paramètres sous l'onglet **Général** de la boîte de dialogue **Propriétés de Serveur virtuel IMAP4 par défaut** (figure 3.1).

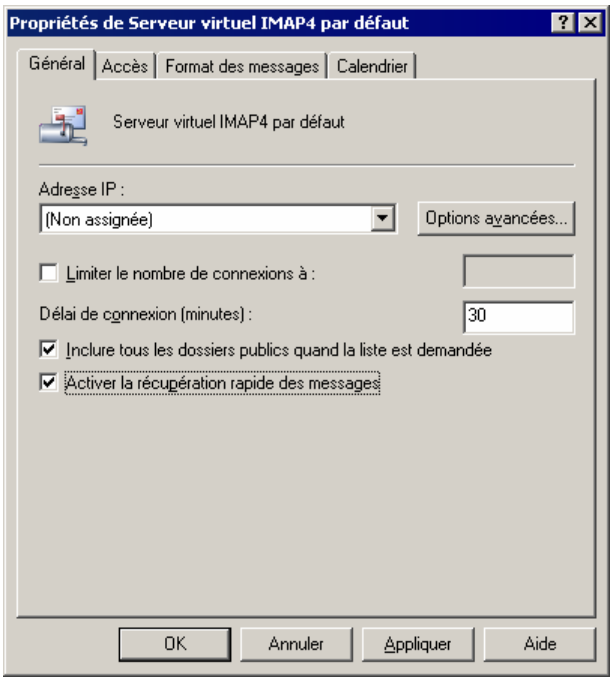

Figure 3.1 Onglet Général de la boîte de dialogue Propriétés de Serveur virtuel IMAP4 par défaut

Configuration des limites de publication NNTP et des paramètres de modération

Exchange Server2003 utilise NNTP pour permettre aux utilisateurs de participer à des groupes de discussion. Il permet également aux utilisateurs qui exécutent des applications clientes prenant en charge le protocole NNTP d'accéder aux dossiers publics de groupes de discussion hébergés sur des ordinateurs Exchange. Les utilisateurs peuvent lire des éléments, tels que des messages et des documents, et les publier sur des groupes de discussion NNTP, qui sont représentés dans Exchange sous la forme de dossiers publics. Par exemple, les utilisateurs peuvent partager des informations en publiant des messages dans le dossier public d'un groupe de discussion correspondant à leur domaine d'intérêt. Les autres utilisateurs peuvent lire ces messages et y répondre dans le groupe de discussion. Les éléments des groupes de discussion peuvent être répliqués sur des ordinateurs hôtes USENET par le biais d'échanges de News.

Un échange de News est un flux d'éléments entre un site USENET et un autre. Les échanges de News permettent aux utilisateurs de différents sites de News de lire et de publier des articles dans des groupes de discussion comme s'ils utilisaient un seul et unique site de News. Un site de News est un ensemble de groupes de discussions associés. Un article publié dans un site de News défini est ainsi transmis à d'autres sites de News où il peut être lu. Vous devez créer un échange de News pour chaque serveur distant auquel vous voulez distribuer des articles de News.

Comme la raison pour l'utilisation de groupes de discussion est la publication et le partage d'informations, vous serez probablement amené à gérer la taille de ces publications en fonction des ressources disponibles sur le serveur virtuel NNTP. Le fait d'accepter des articles trop longs ou des données trop volumineuses pendant une connexion peut accroître le trafic, surcharger le réseau et saturer rapidement votre disque dur. Assurez-vous que la taille limite que vous spécifiez convient aux capacités de votre serveur.

Pour configurer les limites de publication et les paramètres de modération pour un serveur virtuel NNTP

1. Connectez-vous au serveur Exchange sur lequel le serveur virtuel s'exécute, ouvrez une session avec un compte d'administrateur Exchange doté d'autorisations d'administration locales et d'autorisations d'administration intégrales Exchange.

2. Dans le Gestionnaire système Exchange, développez **Protocoles**, cliquez avec le bouton droit sur le protocole pour lequel vous souhaitez modifier les limites de connexion, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Paramètres** (figure 3.2), sélectionnez les options suivantes :
   - Pour permettre aux clients de publier des articles dans les groupes de discussion sur ce serveur virtuel NNTP, sélectionnez **Autoriser les clients à publier**. Cette option permet aux utilisateurs de publier et de lire des articles dans les groupes de discussion auxquels ils ont accès, sauf si le groupe de discussion est en lecture seule. Vous pouvez également limiter la taille de l'article publié par les clients, en plus du volume du téléchargement pour la connexion.
   - Pour permettre aux clients de publier des articles dans les échanges de News sur le serveur virtuel NNTP, sélectionnez **Autoriser les alimentations à publier**. Vous pouvez limiter la taille des articles publiés en utilisant la case à cocher **Limiter la taille de publication**. Vous pouvez limiter le volume de données envoyées à un échange de News au cours d'une seule connexion en utilisant la case à cocher **Limiter la taille de connexion**.

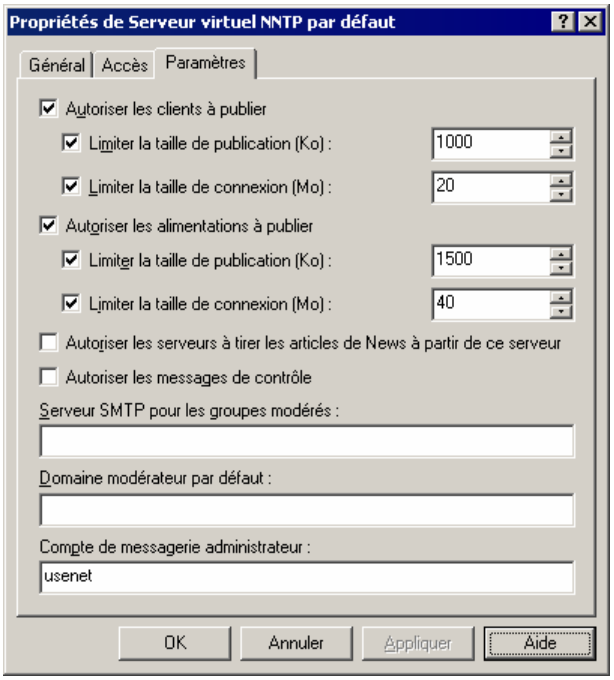

Figure 3.2 Onglet Paramètres de la boîte de dialogue Propriétés de Serveur virtuel NNTP par défaut

Remarque Pour plus d'informations sur la configuration de NTTP, consultez l'aide d'Exchange Server 2003.

Gestion d'Outlook Web Access

Outlook Web Access pour Exchange 2003 comprend des améliorations importantes relatives à l'interface utilisateur et à l'administration. Pour plus d'informations sur les améliorations apportées à la mise en œuvre d'Outlook Web Access, consultez la section « Fonctionnalités client » du manuel *Nouveautés d'Exchange 2003* (http://go.microsoft.com/fwlink/?linkid=21765).

Vous pouvez utiliser aussi bien le Gestionnaire système Exchange que le composant logiciel pour gérer Outlook Web Access. Utilisez :

- le Gestionnaire système Exchange pour modifier les paramètres du contrôle d'accès à Outlook Web Access ;
- le composant logiciel enfichable IIS pour gérer les paramètres d'authentification des répertoires virtuels Outlook Web Access, y compris \Exchange, \Exchweb et \Public ;

- le composant logiciel enfichable IIS pour activer SSL pour Outlook Web Access. Pour plus d'informations sur l'utilisation de SSL avec Outlook Web Access, consultez « Configuration de Microsoft Exchange Server 2003 pour l'accès client » dans le *Guide de déploiement d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

Les sections suivantes indiquent comment utiliser le Gestionnaire système Exchange et le composant logiciel enfichable IIS pour effectuer des tâches de gestion associées à Outlook Web Access.

Activation et désactivation d'Outlook Web Access pour les clients internes uniquement

Vous pouvez accorder aux utilisateurs de votre réseau d'entreprise un accès à Outlook Web Access, et parallèlement refuser l'accès aux utilisateurs externes. En l'occurrence, la solution consiste à combiner une stratégie de destinataire et un serveur virtuel HTTP spécial. Les étapes de cette procédure sont les suivantes :

1. Créez une stratégie de destinataire avec un nom de domaine SMTP. Les utilisateurs connectés à un serveur virtuel HTTP doivent avoir une adresse électronique avec le même domaine SMTP en tant que serveur virtuel. Le fait de créer une stratégie de destinataire est un moyen efficace pour appliquer le même domaine SMTP à plusieurs utilisateurs.

   Remarque Les utilisateurs Outlook Web Access n'ont pas besoin de connaître le nom du domaine SMTP.
2. Appliquez la stratégie de destinataire aux comptes d'utilisateur pour lesquels vous souhaitez activer l'accès.
3. Ensuite, sur le serveur frontal, créez un nouveau serveur virtuel HTTP qui spécifie le domaine utilisé dans la stratégie de destinataire.

Après que vous avez effectué ces étapes, les utilisateurs dont les adresses de messagerie n'ont pas le même domaine SMTP que le serveur virtuel HTTP ne pourront pas se connecter et accéder à Outlook Web Access. Par ailleurs, tant que vous n'utilisez pas le domaine SMTP en tant que domaine par défaut, les utilisateurs externes ne peuvent pas déterminer le domaine SMTP parce que le domaine n'apparaît pas dans le champ **De** lorsque les utilisateurs envoient des messages électroniques à l'extérieur de l'organisation.

Remarque Pour plus d'informations sur les utilisateurs avec boîte aux lettres ayant une adresse SMTP qui n'est pas en relation avec l'adresse spécifiée dans la stratégie de destinataire par défaut, consultez l'article 257891 de la Base de connaissances Microsoft, « XWEB: 'The Page Could Not Be Found' Error Message When You Use OWA » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=257891).

Outre le fait d'activer Outlook Web Access pour les utilisateurs au sein de votre réseau d'entreprise, vous pouvez également empêcher des utilisateurs internes déterminés d'accéder à Outlook Web Access. Pour ce faire, vous pouvez désactiver les protocoles HTTP et NNTP pour ces utilisateurs.

Pour empêcher un utilisateur interne d'accéder à Outlook Web Access

1. Dans Utilisateurs et ordinateurs Active Directory, ouvrez la boîte de dialogue **Propriétés** de l'utilisateur.
2. Sous l'onglet **Fonctionnalités Exchange**, désactivez les paramètres associés à HTTP et NNTP.

Utilisation des paramètres de la langue du navigateur

Lorsque vous utilisez Microsoft Internet Explorer 5 ou version ultérieure pour accéder à Outlook Web Access, les nouvelles installations et mises à niveau de Microsoft Exchange 2003 utilisent les paramètres de langue du navigateur pour déterminer le jeu de caractères à utiliser pour coder les informations comme les messages électroniques et les demandes de réunion.

Si vous effectuez la mise à niveau d'un serveur hébergeant Exchange 2000 qui a été modifié pour utiliser un paramètre de langue d'un navigateur, Exchange 2003 continue à fonctionner de la même manière. Le tableau 3.2 répertorie les groupes de langues et les jeux de caractères correspondants.

Tableau 3.2 Groupe de langues et jeux de caractères Outlook Web Access

Groupe de langues	Jeu de caractères
Arabe	Windows 1256
Balte	iso-8859-4
Chinois (simplifié)	Gb2131
Chinois (traditionnel)	Big5
Cyrillique	koi8-r
Europe de l'est	iso-8859-2
Grec	iso-8859-7
Hébreu	windows-1255
Japonais	iso-2022-jp
Coréen	ks_c_5601-1987
Thaïlandais	windows-874
Turc	iso-8859-9
Vietnamien	windows-1258
Europe de l'ouest	iso-8859-1

Si vous pensez que les utilisateurs Outlook Web Access de votre organisation enverront du courrier fréquemment, vous pouvez modifier les paramètres du Registre pour que les utilisateurs qui exécutent Internet Explorer 5 ou version ultérieure puissent utiliser les caractères Unicode codés par UTF-8 pour envoyer le courrier.

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données utiles.

Pour modifier le paramètre de langue par défaut pour Outlook Web Access

1. Sur le serveur Exchange, ouvrez une session avec le compte d'administrateur Exchange et démarrez l'Éditeur du Registre (**regedit**).
2. Dans l'Éditeur du Registre, recherchez la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   MSExchangeWEB\OWA\UseRegionalCharset
   ```
3. Créez une valeur DWORD nommée **UseRegionalCharset**.

4. Cliquez avec le bouton droit sur la valeur DWORD **UseRegionalCharset**, puis cliquez sur **Modifier**.
5. Dans **Édition de la valeur DWORD**, dans la zone **Données de la valeur**, tapez **1**, puis cliquez sur **OK**.
6. Fermez l'Éditeur du Registre pour enregistrer les modifications.

Blocage des balises Web

Dans Exchange 2003, Outlook Web Access complique la tâche des personnes qui envoient des messages électroniques indésirables afin d'utiliser des balises pour récupérer des adresses de messagerie. Les balises se présentent fréquemment sous la forme d'images qui sont téléchargées sur l'ordinateur d'un utilisateur lorsque celui-ci ouvre un élément de courrier indésirable. Une fois les images téléchargées, un signal est envoyé à l'expéditeur du courrier indésirable pour l'informer que l'adresse de messagerie de votre utilisateur est valide. Il en résulte que l'utilisateur recevra des courriers indésirables plus fréquemment car l'expéditeur est désormais informé que son adresse de messagerie est valide.

Dans Outlook Web Access, un message entrant dont le contenu peut être utilisé comme balise, que ce message contienne réellement une balise ou non, entraîne l'affichage par Outlook Web Access du message d'avertissement suivant :

> Pour protéger la confidentialité, les liens aux images, sons ou autre contenu externe dans ce message ont été bloqués. Cliquer ici pour débloquer le contenu.

Si les utilisateurs savent que le message considéré est légitime, ils peuvent cliquer sur le lien **Cliquer ici pour débloquer le contenu** dans le message d'avertissement et débloquer le contenu. S'ils ne reconnaissent pas l'expéditeur ni le message, ils peuvent ouvrir le message sans débloquer le contenu, puis supprimer le message sans déclencher les balises. Si votre organisation ne souhaite pas utiliser cette fonctionnalité, vous pouvez désactiver l'option de blocage d'Outlook Web Access.

Pour désactiver l'option de blocage

- À la page **Options** d'Outlook Web Access de l'utilisateur, sous **Confidentialité et prévention du courrier indésirable**, désactivez la case à cocher **Bloquer le contenu externe dans les messages HTML**.

Configuration du traitement des pièces jointes

Outlook Web Access peut être configuré pour traiter les pièces jointes du courrier électronique en fonction des besoins de votre organisation. Vos serveurs Exchange peuvent traiter les pièces jointes selon trois méthodes différentes :

1. ne pas autoriser les pièces jointes ;
2. autoriser les pièces jointes (en attente d'un filtrage par type de fichier) ;
3. autoriser l'accès aux pièces jointes uniquement via des serveurs principaux spécifiques.

De plus, vous pouvez spécifier une liste de serveurs frontaux qui font exception à l'option d'autorisation d'accès aux pièces jointes via des serveurs principaux, permettant ainsi aux utilisateurs qui se connectent via les serveurs frontaux spécifiés de pouvoir accepter les pièces jointes. Il est à noter que si vous paramétrez le serveur pour qu'il autorise toutes les pièces jointes ou pour qu'il n'en autorise aucune, cette valeur sera ignorée. Par ailleurs, si une requête est présentée via un serveur frontal spécifié dans la liste des serveurs frontaux qui acceptent les pièces jointes, les pièces jointes doivent encore répondre aux restrictions des niveaux 1 et 2.

Blocage des pièces jointes

Avec Outlook Web Access, vous pouvez empêcher les utilisateurs d'ouvrir, d'envoyer ou de recevoir des types précis de pièces jointes. Plus précisément, vous pouvez :

- **Empêcher les utilisateurs d'accéder aux pièces jointes d'un certain type** Par défaut, toutes les nouvelles installations Exchange 2003 bloquent les pièces jointes de types fichier de niveaux 1 et 2, et de type MIME de niveaux 1 et 2. Cette fonctionnalité s'avère particulièrement efficace pour empêcher les utilisateurs Outlook Web Access d'ouvrir des pièces jointes sur des terminaux Internet publics, ce qui est

susceptible de compromettre la sécurité de l'entreprise. Si une pièce jointe est bloquée, un message d'avertissement indiquant que l'utilisateur ne peut pas ouvrir la pièce jointe apparaît dans la barre d'information du message électronique.

Les utilisateurs Outlook Web Access travaillant dans leurs bureaux ou connectés au réseau d'entreprise à partir de leur domicile peuvent ouvrir et lire les pièces jointes. Vous pouvez activer l'accès intranet intégral aux pièces jointes en indiquant l'URL des serveurs principaux et en autorisant les pièces jointes sur les serveurs principaux Exchange.

- **Empêcher les utilisateurs d'envoyer ou de recevoir des pièces jointes avec des extensions de fichier spécifiques pouvant contenir des virus** Cette fonctionnalité d'Outlook Web Access correspond à la fonctionnalité de blocage des pièces jointes dans Outlook. Pour les messages reçus, un message d'avertissement indiquant qu'une pièce jointe est bloquée s'affiche dans la barre d'information du message électronique. En ce qui concerne les messages envoyés, les utilisateurs ne sont pas autorisés à télécharger des fichiers dont l'extension figure dans la liste d'interdiction.

Pour modifier les paramètres de blocage des pièces jointes, vous devez modifier les paramètres du Registre sur le serveur.

Avertissement Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données utiles.

Pour modifier les paramètres de blocage des pièces jointes sur un serveur Exchange

1. Sur le serveur Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez l'Éditeur du Registre (**regedit**).
2. Dans l'Éditeur du Registre, recherchez la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   MSExchangeWeb\OWA
   ```
3. Dans le menu **Edition**, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.
4. Dans le volet d'informations, nommez la nouvelle valeur **DisableAttachments**.
5. Cliquez avec le bouton droit sur **DisableAttachments**, puis cliquez sur **Modifier**.
6. Sous **Base**, dans **Édition de la valeur DWORD**, cliquez sur **Décimale**.
7. Dans la zone **Données de la valeur**, tapez l'un des chiffres suivants :
   - Pour autoriser toutes les pièces jointes, tapez **0**.
   - Pour désactiver toutes les pièces jointes, tapez **1**.
   - Pour autoriser les pièces jointes provenant uniquement de serveurs principaux, tapez **2**.
8. Cliquez sur **OK**.

Spécification de serveurs frontaux qui autorisent le traitement des pièces jointes

Vous pouvez spécifier une liste de serveurs frontaux et qui font exception à l'option d'autorisation d'accès aux pièces jointes via des serveurs principaux, permettant ainsi aux utilisateurs qui se connectent via les serveurs principaux spécifiés de pouvoir accepter les pièces jointes. Il est à noter que si vous paramétrez le serveur pour qu'il autorise toutes les pièces jointes ou pour qu'il n'en autorise aucune, cette valeur sera ignorée. Par ailleurs, si une requête est présentée via un serveur frontal spécifié dans la liste de serveurs frontaux qui acceptent les pièces jointes, les pièces jointes doivent encore répondre aux restrictions des niveaux 1 et 2.

Pour configurer le traitement des pièces jointes pour Outlook Web Access

1. Sur le serveur Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez l'Éditeur du Registre (**regedit**).

2. Dans l'Éditeur du Registre, recherchez la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   MSExchangeWeb\OWA
   ```

3. Dans le menu **Edition**, pointez sur **Nouveau**, puis cliquez sur **Valeur chaîne**.
4. Dans le volet d'informations, nommez la nouvelle valeur **AcceptedAttachmentFrontEnds**.
5. Cliquez avec le bouton droit sur **AcceptedAttachmentFrontEnds**, puis cliquez sur **Modifier**.
6. Dans **Modification de la chaîne**, sous **Données de la valeur**, entrez les noms des serveurs frontaux qui doivent autoriser les pièces jointes.
7. Cliquez sur **OK**.

Filtrage des messages indésirables

Vous pouvez gérer la façon dont Exchange 2003 gère le courrier électronique indésirable pour votre organisation. Pour ce faire, vous devez activer le filtrage, puis configurer le filtrage de l'expéditeur, du destinataire et de la connexion. Pour plus d'informations sur la gestion des courriers indésirables dans Exchange 2003, consultez la section « Activation du filtrage pour contrôler les messages électroniques indésirables » dans le *Guide de transport et de routage Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=26041).

Gestion d'ActiveSync Exchange

Grâce à ActiveSync Exchange, les utilisateurs de périphériques mobiles Windows dotés du logiciel ActiveSync personnel peuvent synchroniser leurs périphériques avec leurs serveurs Exchange sur Internet. Ils se connectent sur Internet à leur serveur frontal Exchange et demandent les informations à leur serveur de messagerie Exchange. Lorsque vous activez l'accès à Exchange à l'aide d'ActiveSync Exchange, effectuez les étapes ci-dessous.

1. Utilisez l'architecture serveur frontal/principal pour fournir un espace de noms unique aux utilisateurs pour la connexion à votre réseau (recommandé). *Pour plus d'informations, consultez Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766)
2. Installez un certificat SSL sur le serveur frontal. Pour plus d'informations, consultez le *Guide de déploiement* d'*Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).
3. Indiquez aux utilisateurs comment se connecter à Internet à partir de leur périphérique et comment utiliser ActiveSync sur leur périphérique pour se connecter à leur serveur Exchange. Pour plus d'informations, consultez le *Guide de déploiement* d'*Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

Les sections suivantes indiquent comment gérer Exchange ActiveSync pour votre organisation, et notamment comment activer et désactiver l'application Exchange ActiveSync, et comment activer ActiveSync pour vos utilisateurs.

Activation d'ActiveSync Exchange pour votre organisation

Par défaut, ActiveSync Exchange est activé pour tous les utilisateurs de votre organisation. Si vos utilisateurs ont des périphériques mobiles Windows, vous pouvez leur indiquer comment les configurer pour utiliser ActiveSync Exchange. Pour plus d'informations sur la manière d'apprendre à vos utilisateurs à utiliser ActiveSync Exchange, consultez « Configuration de Microsoft Exchange Server 2003 pour l'accès client » dans le *Guide de déploiement d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

Pour activer et désactiver ActiveSync Exchange pour votre organisation, utilisez le Gestionnaire système Exchange. Cependant, lorsque vous ajoutez de nouveaux utilisateurs à votre organisation et que vous souhaitez leur permettre d'utiliser ActiveSync Exchange pour accéder à Exchange avec un périphérique mobile Windows, utilisez Utilisateurs et ordinateurs Active Directory pour redéfinir les paramètres associés à l'utilisateur ou au groupe d'utilisateurs concerné. Les procédures suivantes indiquent comment activer ou désactiver l'application ActiveSync Exchange pour votre organisation et comment modifier les paramètres ActiveSync Exchange pour traiter de nouveaux utilisateurs.

Pour activer ou désactiver ActiveSync Exchange pour votre organisation

1. Sur le serveur frontal Exchange hébergeant ActiveSync Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez le Gestionnaire système Exchange.
2. Développez **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. À la page **Propriétés de Services mobiles**, dans le volet ActiveSync Exchange, activez ou désactivez la case à cocher en regard de l'option **Activer la synchronisation initiée par l'utilisateur**.
4. Cliquez sur **OK**.

Pour modifier les paramètres ActiveSync Exchange

1. Sur le serveur Exchange hébergeant la boîte aux lettres de l'utilisateur, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez Utilisateurs et ordinateurs Active Directory.
2. Développez le domaine, puis ouvrez l'emplacement des utilisateurs que vous souhaitez gérer.
3. Cliquez avec le bouton droit sur l'utilisateur ou sur les utilisateurs dont vous souhaitez modifier les paramètres ActiveSync Exchange, puis sélectionnez **Tâches Exchange**.
4. Dans l'Assistant Tâches Exchange, à la page **Tâches disponibles**, sélectionnez **Configurer Fonctionnalités Exchange**, puis cliquez sur **Suivant**.
5. À la page **Configurer Fonctionnalités Exchange**, sélectionnez **Synchronisation initiée par l'utilisateur**, puis sélectionnez l'une des options suivantes :
   - Pour permettre aux utilisateurs d'utiliser ActiveSync Exchange pour synchroniser leur boîte aux lettres Exchange avec leurs périphériques mobiles, sélectionnez **Activer**.
   - Pour empêcher les utilisateurs d'utiliser ActiveSync Exchange, sélectionnez **Désactiver**.
   - Pour empêcher que les paramètres des utilisateurs soient modifiés lorsque vous avez sélectionné plusieurs utilisateurs, sélectionnez **Ne pas modifier**.
6. Cliquez sur **Suivant** pour appliquer vos modifications.
7. Cliquez sur **Terminer**.

   Remarque Pour consulter un rapport détaillé des paramètres et des modifications que vous avez appliqués aux utilisateurs, sélectionnez **Afficher un rapport détaillé à la fermeture de cet Assistant**.

Activation de notifications actualisées pour votre organisation

Après que vous avez configuré votre organisation pour utiliser ActiveSync Exchange, vous pouvez configurer vos serveurs Exchange 2003 pour que les utilisateurs puissent recevoir des notifications actualisées permettant à leurs périphériques d'être informés lorsqu'un nouvel élément arrive dans leur boîte aux lettres Exchange. Elles invitent le périphérique de l'utilisateur à procéder à une synchronisation automatique avec la boîte aux lettres Exchange.

Pour activer les notifications actualisées pour votre organisation

1. Sur le serveur frontal Exchange hébergeant ActiveSync Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez le Gestionnaire système Exchange.

2. Développez **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. À la page **Propriétés de Services mobiles**, dans le volet ActiveSync Exchange, sélectionnez **Activer les notifications actualisées**.
4. Cliquez sur **OK**.

Pour modifier les paramètres de notifications actualisées de vos utilisateurs

1. Sur le serveur Exchange hébergeant la boîte aux lettres de l'utilisateur, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez Utilisateurs et ordinateurs Active Directory.
2. Développez le domaine, puis ouvrez l'emplacement des utilisateurs dont vous souhaitez modifier les paramètres.
3. Cliquez avec le bouton droit sur l'utilisateur ou sur les utilisateurs dont vous souhaitez modifier les paramètres de notifications actualisées, puis sélectionnez **Tâches Exchange**.
4. Dans l'Assistant Tâches Exchange, à la page **Tâches disponibles**, sélectionnez **Configurer Fonctionnalités Exchange**, puis cliquez sur **Suivant**.
5. À la page **Configurer Fonctionnalités Exchange**, sélectionnez **Notifications actualisées**, puis sélectionnez l'une des options suivantes :
   - Pour permettre aux utilisateurs d'utiliser des notifications actualisées, sélectionnez **Activer**.
   - Pour empêcher les utilisateurs d'utiliser des notifications actualisées, sélectionnez **Désactiver**.
   - Pour empêcher que les paramètres des utilisateurs soient modifiés lorsque vous avez sélectionné plusieurs utilisateurs, sélectionnez **Ne pas modifier**.

Prise en charge des utilisateurs utilisant un opérateur mobile pour la réception de notifications

Si vous activez la fonctionnalité de notifications actualisées ActiveSync Exchange, vos utilisateurs utilisent un opérateur mobile pour transmettre à leurs périphériques les messages provenant du réseau d'entreprise. Vous pouvez autoriser les utilisateurs à recevoir des notifications de deux façons :

Option 1 : Spécifier un opérateur mobile pour vos utilisateurs

Pour spécifier un opérateur mobile pour vos utilisateurs, désactivez **Activer les notifications aux adresses spécifiées par l'utilisateur** sur le serveur Exchange hébergeant les boîtes aux lettres de ces utilisateurs. Si vous sélectionnez cette option, vous devez indiquer à vos utilisateurs comment définir leurs périphériques pour utiliser l'opérateur mobile que vous spécifiez pour les notifications actualisées.

Option 2 : Autoriser les utilisateurs à employer leurs propres opérateurs mobiles

Si vos utilisateurs ont leurs propres périphériques mobiles Windows, vous pouvez les autoriser à utiliser leurs propres opérateurs mobiles pour transmettre des notifications à leurs périphériques. Si vous sélectionnez cette option, vous devez indiquer à vos utilisateurs comment définir leurs périphériques pour utiliser les opérateurs mobiles de leur choix pour les notifications actualisées.

Les deux procédures suivantes précisent comment configurer ces options. La première indique comment définir l'option **Activer les notifications aux adresses SMTP spécifiées par l'utilisateur**, et la seconde comment définir l'opérateur mobile sur le périphérique d'un utilisateur.

Pour définir l'option Activer les notifications aux adresses SMTP spécifiées par l'utilisateur pour votre organisation

1. Sur le serveur frontal Exchange hébergeant ActiveSync Exchange, ouvrez une session avec le compte d'administrateur Exchange, puis démarrez le Gestionnaire système Exchange.
2. Développez **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. À la page **Propriétés de Services mobiles**, dans le volet ActiveSync Exchange, définissez l'option **Activer les notifications aux adresses SMTP spécifiées par l'utilisateur** comme suit :

- Si vous souhaitez définir un opérateur mobile pour votre utilisateur, désactivez l'option **Activer les notifications aux adresses SMTP spécifiées par l'utilisateur**.
- Si vous souhaitez autoriser vos utilisateurs à spécifier leurs propres opérateurs mobiles, activez l'option **Activer les notifications aux adresses SMTP spécifiées par l'utilisateur**.

4. Cliquez sur **OK**.

Pour spécifier un opérateur mobile pour les notifications actualisées sur un périphérique

1. Dans ActiveSync, sur un périphérique mobile Windows, sélectionnez **Outils**, puis **Options**.
2. Sous l'onglet **Serveur**, sélectionnez **Options**.
3. À l'écran **Options de synchronisation serveur**, sélectionnez **Adresse du périphérique**.
4. À l'écran **Adresse du périphérique**, effectuez l'une des opérations suivantes :
   - Si vos utilisateurs utilisent un opérateur mobile que vous spécifiez, sélectionnez **Fournisseur de services d'entreprise**, puis entrez **N° de téléphone de l'appareil** et **Nom du fournisseur de services** dans les champs prévus à cet effet.
   - Si vos utilisateurs utilisent leurs propres opérateurs mobiles, sélectionnez **Adresse SMS de l'appareil**, puis entrez l'adresse du périphérique dans le champ prévu à cet effet.

Gestion d'Outlook Mobile Access

En utilisant Outlook Mobile Access, les utilisateurs peuvent parcourir leur boîte aux lettres Exchange à l'aide d'un périphérique comme Smartphone Microsoft sous Windows ou un périphérique compatible cHTML. Vous pouvez également autoriser les utilisateurs à utiliser des périphériques qui ne sont pas officiellement pris en charge par Microsoft, mais qui peuvent fonctionner correctement avec des problèmes de compatibilité mineurs en autorisant les périphériques non pris en charge à utiliser Outlook Mobile Access.

Les sections suivantes indiquent comment gérer Exchange ActiveSync pour votre organisation, et notamment comment activer et désactiver l'application Exchange ActiveSync, et comment activer ActiveSync pour vos utilisateurs.

Configuration d'Exchange pour l'utilisation d'Outlook Mobile Access

Par défaut, Outlook Mobile Access est désactivé lorsque vous installez Exchange 2003. Pour permettre aux utilisateurs d'utiliser Outlook Mobile Access, vous devez l'activer au préalable. Lorsque vous activez l'accès à Exchange à l'aide d'Outlook Mobile Access, vous devez procéder comme suit :

1. Utilisez l'architecture serveur frontal/principal pour fournir un espace de noms unique aux utilisateurs pour la connexion à votre réseau. Pour plus d'informations, consultez le guide *Using Microsoft Exchange 2000 Front-End Servers* (http://go.microsoft.com/fwlink/?linkid=12055).
2. Installez un certificat SSL sur le serveur frontal. Pour plus d'informations, consultez le *Guide de déploiement* d'*Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).
3. Indiquez aux utilisateurs comment se connecter à Internet à partir de leurs périphériques et comment utiliser Outlook Mobile Access pour accéder aux informations Exchange. Pour plus d'informations, consultez le *Guide de déploiement* d'*Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768).

Activation d'Outlook Mobile Access pour votre organisation

Pour activer Outlook Mobile Access pour vos organisations, utilisez le Gestionnaire système Exchange. Après avoir activé Outlook Mobile Access, vous pouvez utiliser Utilisateurs et ordinateurs Active Directory pour modifier les paramètres Outlook Mobile Access pour des utilisateurs ou pour des groupes d'utilisateurs.

Pour activer Outlook Mobile Access pour votre organisation

1. Ouvrez une session en tant qu'administrateur Exchange avec le serveur Exchange hébergeant la boîte aux lettres de l'utilisateur, puis démarrez le Gestionnaire système Exchange.
2. Développez **Paramètres globaux**, cliquez avec le bouton droit sur **Services mobiles**, puis cliquez sur **Propriétés**.
3. À la page **Propriétés de Services Mobile**, dans le volet Outlook Mobile Access, sélectionnez **Activer Outlook Mobile Access**.
4. Pour permettre aux utilisateurs d'utiliser des périphériques non pris en charge, sélectionnez **Activer les périphériques non pris en charge**.

   Remarque Pour plus d'informations sur les périphériques pris en charge pour Exchange et la planification de la prise en charge de périphériques mobiles avec Exchange, consultez le guide *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766).
5. Cliquez sur **OK**.

Pour modifier les paramètres Outlook Mobile Access

1. Ouvrez une session en tant qu'administrateur Exchange avec le serveur Exchange hébergeant la boîte aux lettres de l'utilisateur, puis démarrez le Gestionnaire système Exchange.
2. Développez le domaine, puis ouvrez l'emplacement des utilisateurs dont vous souhaitez modifier les paramètres.
3. Cliquez avec le bouton droit sur l'utilisateur ou sur les utilisateurs dont vous souhaitez modifier les paramètres Outlook Mobile Access, puis sélectionnez **Tâches Exchange**.
4. Dans l'Assistant Tâches Exchange, à la page **Tâches disponibles**, sélectionnez **Configurer Fonctionnalités Exchange**, puis cliquez sur **Suivant**.
5. À la page **Configurer Fonctionnalités Exchange**, sélectionnez **Outlook Mobile Access**, puis sélectionnez l'une des actions suivantes :
   - Pour permettre aux utilisateurs d'utiliser Outlook Mobile Access, sélectionnez **Activer**.
   - Pour empêcher les utilisateurs d'utiliser Outlook Mobile Access, sélectionnez **Désactiver**.
   - Pour empêcher que les paramètres de l'utilisateur soient modifiés lorsque vous avez sélectionné plusieurs utilisateurs, sélectionnez **Ne pas modifier**.
6. Cliquez sur **Suivant** pour appliquer vos modifications.
7. Cliquez sur **Terminer**.

Annexe

Ressources

Ressources mentionnées dans ce guide

Exchange Server 2003

Documentation technique

- *Exchange Server 2003 RPC over HTTP Deployment Scenarios* (http://go.microsoft.com/fwlink/?linkid=24823)
- *Using Microsoft Exchange 2000 Front-End Servers* (http://go.microsoft.com/fwlink/?linkid=12055)

Articles de la Base de connaissances Microsoft

Les articles de la Base de connaissances Microsoft suivants sont disponibles sur le Web à l'adresse http://go.microsoft.com/fwlink/?linkid=14898

- 320291, « XCCC : Activation de SSL pour Exchange 2000 Server Outlook Web Access » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=320291)
- 257891, « XWEB: The 'Page Could Not Be Found' Error Message When You Use OWA » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=257891)
- 279681, « How to Force SSL Encryption for an Outlook Web Access 2000 Client » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=279681)

Windows 2000

Articles de la Base de connaissances Microsoft

- 233256, « How to Enable IPSec Traffic Through a Firewall » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=233256)

Autres sites Web

- Centre de sécurité Microsoft Exchange Server (http://go.microsoft.com/fwlink/?linkid=18412)

Ressources supplémentaires

Outre les ressources citées dans ce guide, les ressources mentionnées ci-après peuvent vous apporter une aide précieuse pour votre mise en œuvre de Microsoft® Exchange Server 2003.

Sites Web

- Compatibilité Exchange 2003 avec les périphériques mobiles (http://go.microsoft.com/fwlink/?linkid=24847)
- Bibliothèque technique de Microsoft Exchange Server 2003 (http://go.microsoft.com/fwlink/?linkid=21277)

- Outils et mises à jour Exchange Server 2003 (http://go.microsoft.com/fwlink/?linkid=25097)
- Exchange Server 2003 Glossary (http://go.microsoft.com/fwlink/?linkid=24625)
- Microsoft Developer Network (MSDN®) (http://go.microsoft.com/fwlink/?linkid=21574)
- Correctif cumulatif pour Internet Explorer (328970) (http://go.microsoft.com/fwlink/?linkid=16694).
- Site Web de sécurité Microsoft (http://go.microsoft.com/fwlink/?linkid=21633)
- Site Web de sécurité TechNet (http://go.microsoft.com/fwlink/?LinkID=5936)
- Site Web des services de support technique de Microsoft (http://go.microsoft.com/fwlink/?linkid=14898).

Manuels consacrés à Exchange Server 2003

- Nouveautés d'Exchange 2003 (http://go.microsoft.com/fwlink/?linkid=21765)
- *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com.fwlink/?linkid=21766)
- *Guide de déploiement de Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21768)
- *Guide de déploiement de Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=26041)

Kits de ressources

- *Kit de ressources Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?linkid=12058)

  Remarque Vous pouvez commander un exemplaire du *Kit de ressources Microsoft Exchange 2000 Server* auprès de Microsoft Press® à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=6544.

- *Kits de ressources Windows 2000* (http://go.microsoft.com/fwlink/?LinkId=6545)

  Remarque Vous pouvez commander un exemplaire du *Kit de Ressources Techniques Microsoft Windows 2000 Server* auprès de Microsoft Press® à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=6546.

Accessibilité

Pour plus d'informations sur l'accessibilité pour les personnes atteintes de handicaps, consultez le site Web de Microsoft sur l'accessibilité à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=22010.