iPhone en entreprise
Exchange ActiveSync

Règles de sécurité Exchange ActiveSync prises en charge

- Effacement à distance
- Appliquer le mot de passe sur l'appareil
- Nombre minimum de caractères
- Nombre maximum de tentatives (avant effacement local)
- Exiger à la fois des chiffres et des lettres
- Délai d'inactivité en minutes (de 1 à 60 minutes)

Règles Exchange ActiveSync supplémentaires (pour Exchange 2007 et 2010 seulement)

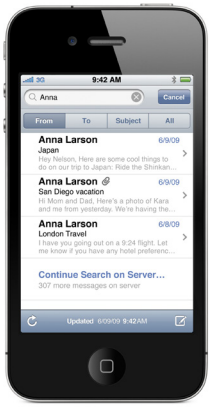
- Autoriser ou interdire les mots de passe simples
- Expiration du mot de passe
- Historique des mots de passe
- Intervalle d'actualisation des règles
- Nombre minimum de caractères complexes dans le mot de passe
- Exiger la synchronisation manuelle pendant l'itinérance
- Autoriser l'appareil photo
- Autoriser la navigation Web

iPhone communique directement avec votre serveur Microsoft Exchange via Microsoft Exchange ActiveSync (EAS), autorisant la transmission en mode "push" du courrier électronique, des calendriers et des contacts. Exchange ActiveSync fournit également aux utilisateurs l'accès à la Liste d'adresses globales et aux administrateurs des capacités de mise en œuvre de politiques de code d'appareil et d'effacement à distance. iPhone prend en charge l'authentification tant de base que par certificat pour Exchange ActiveSync. Si votre entreprise a actuellement Exchange ActiveSync activé, elle a déjà les services nécessaires en place pour prendre en charge iPhone — aucune configuration supplémentaire n'est requise. Si vous avez Exchange Server 2003, 2007 ou 2010 mais que votre société découvre Exchange ActiveSync, suivez les étapes ci-dessous.

Configuration d'Exchange ActiveSync

Présentation de la configuration du réseau

- Assurez-vous que le port 443 est ouvert sur le coupe-feu. Si votre entreprise utilise Outlook Web Access, le port 443 est probablement déjà ouvert.
- Vérifiez qu'un certificat de serveur est installé sur le serveur frontal et activez le protocole SSL pour le répertoire virtuel Exchange ActiveSync dans IIS.
- Si un serveur Microsoft Internet Security and Acceleration (ISA) est utilisé, vérifiez qu'un certificat de serveur est installé et mettez à jour le serveur DNS public de manière à ce qu'il résolve les connexions entrantes.
- Assurez-vous que le DNS de votre réseau retourne une adresse unique routable en externe au serveur Exchange ActiveSync pour les clients intranet et Internet. C'est obligatoire afin que l'appareil puisse utiliser la même adresse IP pour communiquer avec le serveur lorsque les deux types de connexions sont actives.
- Si vous utilisez un serveur Microsoft ISA, créez un écouteur web ainsi qu'une règle de publication d'accès au client web Exchange. Consultez la documentation de Microsoft pour plus de détails.
- Pour tous les coupe-feu et équipements réseau, définissez à 30 minutes le délai d'attente en cas de session inactive. Pour en savoir plus sur les autres intervalles de pulsations et de délai d'attente, consultez la documentation Microsoft Exchange à l'adresse http://technet.microsoft.com/en-us/library/cc182270.aspx.
- Configurez les fonctionnalités, les stratégies et les réglages en matière de sécurité des appareils mobiles à l'aide d'Exchange System Manager. Pour Exchange Server 2007 et 2010, il faut utiliser la console de gestion Exchange.
- Téléchargez et installez l'outil Microsoft Exchange ActiveSync Mobile Administration Web Tool, qui est nécessaire afin de lancer un effacement à distance. Pour Exchange Server 2007 et 2010, un effacement à distance peut aussi être lancé à l'aide d'Outlook Web Access ou de la console de gestion Exchange.



Autres services Exchange ActiveSync

- Consultation de la liste d'adresses globale (GAL)
- Acceptation et création d'invitations dans le calendrier
- Synchronisation des repères Répondre et Transférer à l'aide d'Exchange Server 2010
- Recherche de courrier électronique sur Exchange Server 2007 et 2010
- Prise en charge de plusieurs comptes Exchange ActiveSync
- Authentification par certificats
- Envoi de courrier électronique en mode "push" vers des dossiers sélectionnés
- Découverte automatique

Authentification de base (nom d'utilisateur et mot de passe)

- Activer Exchange ActiveSync pour certains utilisateurs ou groupes à l'aide du service Active Directory. Ces fonctionnalités sont activées par défaut sur tous les appareils mobiles au niveau organisationnel dans Exchange Server 2003, 2007 et 2010. Pour Exchange Server 2007 et 2010, voir l'option Configuration du destinataire dans la console de gestion Exchange.
- Par défaut, Exchange ActiveSync est configuré pour l'authentification de base des utilisateurs. Il est recommandé d'activer le protocole SSL pour l'authentification de base afin que les références soient chiffrées lors de l'authentification.

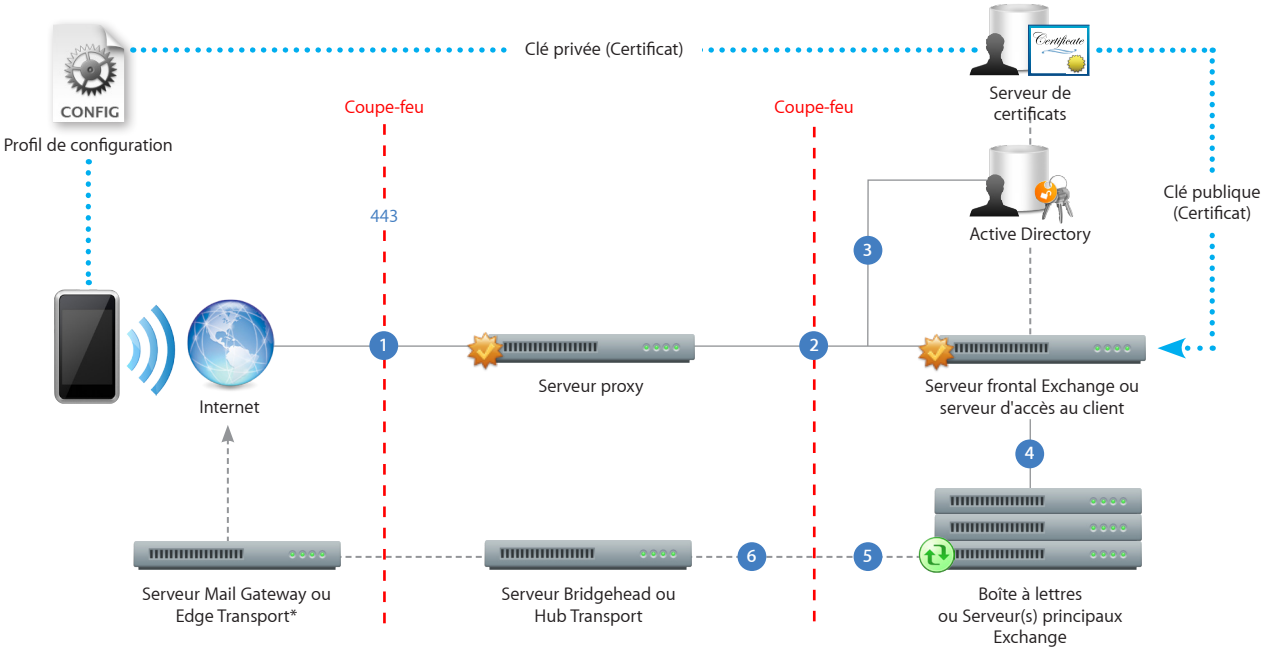
Authentification par certificats

- Installez les services de certificats d'entreprise sur un contrôleur de domaine ou un serveur membre de votre domaine (celui-ci sera votre serveur d'autorité de certification).
- Configurez IIS sur votre serveur frontal Exchange ou votre Serveur d'Accès Client afin d'accepter l'authentification par certificats pour le répertoire virtuel Exchange ActiveSync.
- Pour autoriser ou exiger des certificats pour tous les utilisateurs, désactivez "Authentification de base" et sélectionnez "Accepter les certificats clients" ou "Exiger les certificats clients".
- Générez les certificats clients au moyen de votre serveur d'autorité de certification. Exportez la clé publique et configurez IIS de manière à utiliser cette clé. Exportez la clé privée et utilisez un Profil de configuration pour fournir cette clé à iPhone. L'authentification par certificats peut uniquement être configurée à l'aide d'un Profil de configuration.

  Pour plus d'informations sur les services de certificats, veuillez vous reporter aux ressources disponibles auprès de Microsoft.

Scénario de déploiement d'Exchange ActiveSync

Cet exemple montre comment iPhone se connecte à un déploiement Microsoft Exchange Server 2003, 2007 ou 2010 standard.



*Selon la configuration de votre réseau, le serveur Mail Gateway ou Edge Transport peut résider dans la zone démilitarisée (DMZ).

1. iPhone demande l'accès aux services Exchange ActiveSync via le port 443 (HTTPS). (Il s'agit du même port utilisé pour Outlook Web Access et d'autres services web sécurisés. Dans de nombreux déploiements, ce port est donc déjà ouvert et configuré pour autoriser un trafic HTTPS avec chiffrement SSL.)
2. ISA offre un accès au serveur frontal Exchange ou au serveur d'accès au client. ISA est configuré comme un proxy ou, dans de nombreux cas, comme un proxy inverse, pour acheminer le trafic vers le serveur Exchange.
3. Le serveur Exchange identifie l'utilisateur entrant à l'aide du service Active Directory et du serveur de certificats (si vous utilisez une authentification par certificats).
4. Si l'utilisateur saisit les informations d'identification correctes et a accès aux services Exchange ActiveSync, le serveur frontal établit une connexion à la boîte de réception correspondante sur le serveur principal (via le catalogue global Active Directory).
5. La connexion Microsoft Exchange ActiveSync est établie. Les mises à jour/modifications sont envoyées en mode "push" ('Over The Air' OTA) sur iPhone, et les modifications effectuées sur iPhone sont répercutées sur le serveur Exchange.
6. Les courriers électroniques envoyés depuis l'iPhone sont également synchronisés avec le serveur Exchange via Exchange ActiveSync (étape 5). Pour acheminer le courrier électronique sortant vers des destinataires externes, celui-ci est généralement envoyé par le biais d'un serveur Bridgehead (ou Hub Transport) vers une passerelle Mail (ou Edge Transport) externe via SMTP. Selon la configuration de votre réseau, la passerelle Mail ou le serveur Edge Transport externe peut résider dans la zone démilitarisée ou à l'extérieur du coupe-feu.

 Juin 2010 L419822A