Le serveur de communication IceWarp

Guide Exchange ActiveSync

Version 10.4

Septembre 2013

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Sommaire

Guide Exchange ActiveSync 2

© IceWarp France / DARNIS Informatique

Toute reproduction interdite sans accord d'IceWarp France

Guide Exchange ActiveSync

Introduction

Ce document traite du logiciel de synchronisation **ActiveSync** et de la façon de le configurer pour synchroniser les données entre un appareil **mobile** et le serveur **IceWarp**.

Les **utilisateurs** d'un mobile utilisant ActiveSync et qui souhaitent configurer leur mobile, peuvent aller directement au chapitre Configuration du mobile. Les autres chapitres s'adressent plutôt à **l'administrateur** du serveur IceWarp.

Présentation de Exchange ActiveSync

Exchange ActiveSync (EAS) est un protocole de synchronisation de données propriétaire créé par Microsoft pour la synchronisation de dispositifs mobiles sans fil avec le Serveur Exchange.

IceWarp a acquis une licence de ce protocole qui lui permet de faire une synchronisation de l'iPhone et des mobiles Windows sans nécessiter l'installation d'un quelconque logiciel, réduisant ainsi la durée de déploiement et permettant de nombreuses fonctionnalités non disponibles avec le protocole SyncML.

Exchange ActiveSync est optimisé pour travailler à la fois avec un temps de réaction faible et des réseaux à faible largeur de bande typiques des mobiles. Le protocole, basé sur HTTP et XML, permet aux mobiles d'avoir un accès centralisé via le Serveur IceWarp aux informations les plus importantes de l'organisation. IceWarp avec ActiveSync permettent aux utilisateurs de mobiles d'avoir accès à leur courrier électronique, calendrier, contacts et tâches quand ils sont connectés par le réseau mobiles et aussi d'avoir accès à ces informations pendant qu'ils sont en mode autonome.

Voici quelques précisions pour éviter toute ambiguïté. L'application ActiveSync des postes de travail (le Centre de Communication de Windows Vista) utilise un protocole de communication basé sur XML pour synchroniser des dispositifs connectés localement (Bluetooth ou USB). De même iSync du Mac OS X utilise un protocole SyncML propriétaire pour la synchronisation de dispositifs connectés localement à l'ordinateur de l'utilisateur. Aucun de ces protocoles n'est supporté par le Serveur IceWarp.

© IceWarp France / DARNIS Informatique

Toute reproduction interdite sans accord d'IceWarp France

Marques et recours

Windows, Vista, Exchange, SQL Server, ActiveSync, AutoDiscover, DirectPush, RemoteWipe sont des marques déposées de Microsoft Corporation. BlackBerry, BIS (BlackBerry Internet Service), BES (BlackBerry Enterprise Server) sont des marques déposées de Research In Motion Inc. iPhone, iSync, Mac, OS X sont des marques déposées d'Apple Inc. Symbian est une marque déposée de Symbian Software Ltd. Palm, Palm OS, WebOS sont des marques déposées de Palm Inc. Android est une marque déposée de Google Inc. Nokia for Exchange est une marque déposée de Nokia Corporation. NotifySync est une marque déposée de Notify Corp. AstraSync est une marque déposée de MailSite Software Inc. Moxier est une marque déposée de Emtrace Technologies, Inc. MySQL est une marque déposée de MySQL AB.

Pour toute aide ou information sur les produits mentionnés ci-dessus, pour toute difficulté légale ou privée résultant de leur utilisation, contactez les vendeurs respectifs ou consultez leurs sites Web.

Compatibilités

Exchange ActiveSync est supporté directement par un grand nombre de mobiles :

- Windows CE, PocketPC
- Windows Smartphone
- Windows Mobile 5, 6
- iPhone OS X
- Nokia phones avec Symbian S60, S90 (firmware les plus récents)
- Palm OS 4
- Palm WebOS
- Google Android (certains modèles)

Si ActiveSync n'est pas directement supporté, un logiciel tiers doit être installé sur le mobile pour permettre la synchronisation avec ActiveSync :

- Anciennes versions des séries Nokia N, E, S60 v3: **Mail for Exchange** (Téléchargement gratuit Nokia)
- Symbian S60/S80/S90/UIQ: **DataViz RoadSync**
- BlackBerry: **Notify Corp NotifySync** (OS 4.0 et au delà), **MailSite Software AstraSync** (OS 4.2 et au delà – séries 8xxx, 9xxx)
- Android OS: **Exchange** par **Touchdown** ou **Moxier Mail** par **Emtrace Technologies**
- Motorola avec Java MIDP 2.0: **DataViz RoadSync**

Voir la matrice de compatibilité plus loin dans ce chapitre.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Caractéristiques

ActiveSync permet les synchronisations suivantes (ces informations ne sont pas forcément supportées par le mobile lui même) :

- Emails
- Contacts
- Calendriers
- Tâches
- Push direct toujours actif pour les emails, les contacts, les calendriers et les tâches.

Caractéristiques avancées et gestion du mobile :

- Synchronisation de la structure complète des dossiers

  Tous dossiers, y compris les dossiers partagés et publics

  Affichage des dossiers non email dans la structure IMAP

  Synchronisation des dossiers multiples si le mobile le permet

  Dossiers sélectionnés pour la synchronisation avec des applications internes

- Gestion des dossiers (uniquement sur Windows mobile 6.0 et plus)

  Ajout, suppression, renommage, déplacement dans l'arbre des dossiers

- Manipulation complète des emails (envoi, réponse, transfert, marquage...)
- Manipulation des fichiers attachés (y compris sur les plateformes Windows)
- Utilisation de filtres (synchronisation définie par l'utilisateur)

  Synchronisation des messages ayant moins d'un certain nombre de jours

  Synchronisation des messages inférieurs à une taille donnée ou sans pièce jointe

  Synchronisation d'événements ayant moins d'un certain nombre de jours

  Synchronisation des tâches non marquées terminées

- Gestion du mobile

  Liste de tous les mobiles connectés par domaine/utilisateur avec le nom du modèle

  Effacement distant du mobile pour supprimer toutes les données d'un mobile volé

- Consultation à distance d'un annuaire d'entreprise (GAL)

  Auto complétion des adresses mail

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Consultation des adresses des contacts

- Découverte automatique

  Pour simplifier la configuration, en entrant seulement le nom et le mot de passe du compte

- SmartSync

  Permet de récupérer intelligemment une connexion lorsqu'une erreur s'est produite pendant la réponse du serveur à une demande client

- Réception d'une invitation à une réunion et possibilité d'accepter/refuser

  Seulement pour les réunions créées sur le Client Web ou un client approprié

- Stratégies de sécurité

  Pour renforcer le mot de passe du mobile, le nombre maximum de tentatives mauvaises, l'effacement local du mobile en cas de compromission.

Limitations actuelles

- EAS 2.5 seulement, les mobiles avec 12.1 sont traités en mode 2.5
- EAS 12.0 AutoDiscover et pièces jointes seulement
- EAS 12.1 la synchronisation de base seulement est supportée
- Les invitations aux réunions au format TNEF (envoyées par Outlook) ne sont pas supportées (il n'est pas possible d'y répondre par EAS ni par le Client Web d'IceWarp)
- Les fonctions spécifiques de EAS 12.1 ne sont pas supportées (Exchange 2007: résolution du destinataire et décryptage en S/MIME, téléchargement sélectif de fichiers attachés, provisions pour extensions de la sécurité, récupération de mots de passe, recherche booléenne)
- La configuration hors bureau n'est pas supportée
- Les mails HTML sont transformés en texte pour les mobiles Windows

Avantages sur SyncML

- Fonctionnalités natives pour un grand nombre de mobiles
- Fonctions de gestion du mobile
- Push sur TCP/IP
- Accès aux dossiers partagés

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

- Synchronisation de dossiers multiples sur certains mobiles

Avantages du push direct

- Notification immédiate des messages
- Adapté aux connexions lentes (GSM, WAP, EDGE)
- Les messages sont téléchargés en arrière plan à leur arrivée
- Pas de charges financières liées aux alertes par SMS

Avantages de SmartSync

- Termine simplement une synchronisation qui aurait été réinitialisée sinon
- Préserve les données, du temps et la vie de la batterie
- Préserve la cohérence des données et résolvant les conflits
- Évite les boucles infinies sur des erreurs de synchronisation
- Adapté aux réseaux présentant une mauvaise qualité de connexion

Accès Boîtes aux lettres et GroupWare

- Accès aux fichiers, notes, tâches par l'application de messagerie
- Synchronisation unidirectionnelle du serveur vers le mobile
- Indépendant de la taille limite des mails
- Pas d'applications nécessaires, fonctionne dès la mise en route
- Configuration simple
- Accès sécurisé par SSL (HTTPS)

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Matrice de compatibilité

	Windows mobile Windows PocketPC Windows Smartphone	iPhone iPhone 3G	Série Nokia N Série Nokia E	palm OS 4, 5	Palm Web OS
Plugin	Non	Non	Non - Mail for Exchange (gratuit)	Non	Non
Email	o	o	o	o	o
Calendrier	o	o	o	o	o
Contacts	o	o	o	o	o
Tâches	o	-	o	o	o
Push direct	o**	o	o	o	o
Push programmé	-	-	o	-	-
Consultation GAL	o	o	o	o	o
Sous dossiers	o	o***	-	-	o
Gestion des dossiers	6.x	-	-	-	-
Filtres email/ calendriers/ tâches	o/o/o	o/o/-	o/o/o	o/o/-	o/o/o
Auto découverte	o**	o	-	-	-
Effacement distant	o	o	o	-	-
Sécurité	o	o	o	-	-
iMIP (réponse à convocation)	o	o	o	o	-

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

	Android TouchDown	Android Moxier	BlackBerry NotifySync	BlackBerry AstraSync	Symbian S60, S80, S90, UIQ RoadSync
Plugin	Oui NitroDesk TouchDown	Oui Moxier Mail	Oui NotifySync	Oui AstraSync	Oui DataViz** RoadSync
Email	o	o	o	o	o
Calendrier	o	o	o	o	o
Contacts	o	o	o	o	o
Tâches	o	o	o	-	-
Push direct	o	o	o	o	-
Push programmé	o	o	o	o	o
Consultation GAL	o	o	o	o	o
Sous dossiers	o	o	o	o	-
Gestion des dossiers	-	-	-	-	-
Filtres email, calendriers, tâches	o/o/o	o/o/o	o/o/-	o/o/-	o/o/-
Auto découverte	-	o	-	3.x	-
Effacement distant	o	-	o	3.x	o
Sécurité	o	-	o	3.x	o
iMIP (réponse à convocation)	o	-	o	3.x	o

o disponible

- non disponible

* Le support du push direct n'est disponible que sur les PDA et Smartphones qui tourne sous Windows mobile 5.0 et au delà avec le pack Messaging and Security (MSFP/AKU2). De plus, pour que le push direct et la découverte intelligente fonctionne correctement, un certificat valide doit être installé sur le mobile.

** RoadSync est déjà installé sur certains LG, Nokia, Samsung et Sony Ericsson, et il peut être installé sur la plupart des mobiles Symbian. RoadSync beta est aussi disponible pour Android. RoadSync (messagerie uniquement) est aussi disponible pour les mobiles Motorola Java MIDP 2.0 (RAZR, KRZR...) et les mobiles sous Palm OS.

*** L'iPhone supporte les dossiers multiples (groupes) pour les mails, contacts, événements mais ne supporte pas la modification des dossiers.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Configuration du serveur

Le module ActiveSync du serveur IceWarp est très facile à configurer puisqu'il offre très peu de contrôle d'administration.

1. Dans le menu **Aide -> licence**, vérifier que la **licence** est valide pour au moins un jeton. Si la durée de garantie est dépassée, vous devez obtenir une mise à jour de la licence. Si vous avez des difficultés à gérer les licences, voir cette FAQ.

2. Dans le menu **Système -> Services -> Web**, vérifier que le service tourne

   Ouvrez les propriétés de ce service et vérifiez que les ports spécifiés sont les **ports 80** et 443 (SSL). Si ce n'est pas le cas, modifiez-les et redémarrer le service. Si le service ne redémarre pas, c'est sans doute qu'il y a un conflit avec un autre service du serveur utilisant le même port (MS IIS par exemple) ; dans ce cas, il faut arrêter ce service ou changer son port. ActiveSync ne peut fonctionner qu'avec un service Contrôle sur le port 80 et la découverte automatique ne peut fonctionner qu'avec le port 443.

3. Pour l'accès à la **liste d'adresse globale** (GAL), vous devez avoir un dossier public marqué GAL ou le GAL sera constitué de tous les utilisateurs du serveur. Vois le paragraphe sur les dossiers publics GAL pour plus de détails.

4. Dans le menu **Système -> Services -> IMAP**, vérifiez que le service tourne et que les ports spécifiés sont les ports 143 et 993 (SSL).

5. Dans le menu **Web -> onglet Général** ouvrez le serveur Web actif et aller sur l'onglet Scripting. Vérifiez que les extensions [activesync] et [autodiscover] sont bien associées à **(fastcgi);php\php.exe**. Pour plus de détails, voir la section sur les pannes.

6. Dans le menu **GroupWare -> ActiveSync** modifier uniquement le nom d'hôte si la configuration le nécessite. L'URL doit être de la forme " https://<serveur>/Microsoft-Server-ActiveSync".

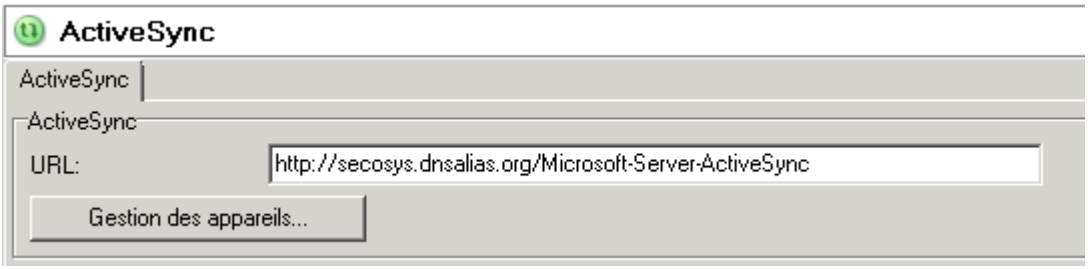
7. Dans **l'onglet Stratégies du compte** utilisateur, vérifier que la case ActiveSync est bien cochée.

8. Pour la découverte automatique (**AutoDiscover**), allez dans **Système -> Services -> onglet SmartDiscover**. Vérifiez que l'URL qui apparaît dans URL -> MobileSync (ActiveSync) est la même que celle qui est dans le menu GroupWare -> ActiveSync. Pour plus de détails, voir le paragraphe sur la Découverte intelligente.

9. Pour augmenter la sécurité et améliorer la performance du push direct et de la découverte intelligente, installez sur le serveur un **certificat signé** par une autorité de certification telle que Verisign par exemple.

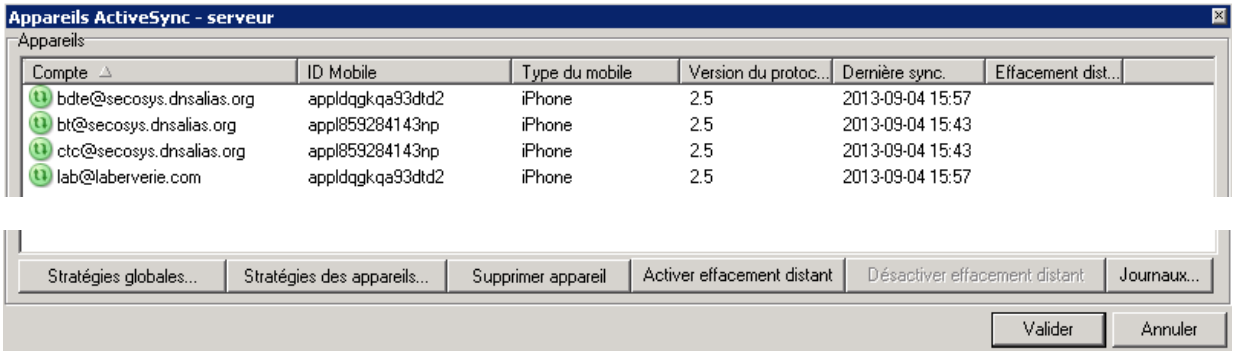
© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Menu GroupWare -> ActiveSync



Champ	Description
URL	L'URL est constituée : • De l'adresse du serveur ou son alias : iwdemo.fr dans l'exemple ci-dessus Ce nom doit être configuré dans le client avec le même nom sinon, la synchronisation ne fonctionnera pas. Note : le port par défaut (80 pour HTTP, 443 pour HTTPs) n'est pas mentionné. l'utilisation d'autres ports pour ce service ne fonctionne pas. • Du chemin spécifié par Microsoft : Microsoft-Server-ActiveSync Note : cette partie de l'URL ne peut pas être modifiée. Elle est indiquée uniquement pour faciliter la recherche des problèmes lors de l'examen des journaux. cette partie de l'URL ne doit pas être indiquée sur le mobile.
Gestion des appareils	Ce bouton fait apparaître la liste des des mobiles qui utilisent ActiveSync - voir ci-dessous.

Bouton "Gestion des appareils" :



© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Bouton	Description
Stratégies globales	Permet de configurer la stratégie de sécurité pour tous les mobiles au niveau du serveur. Pour plus de détails, voir le paragraphe sur les stratégies de sécurité.
Stratégies des appareils	Permet de configurer la stratégie de sécurité pour le mobile sélectionné. Pour plus de détails, voir le paragraphe sur les stratégies de sécurité.
Supprimer appareil	Cette action enlève le mobile de la base de données ActiveSync et va provoquer une resynchronisation complète lors de la prochaine synchronisation automatique ou manuelle. Cette option peut être utilisée lors d'erreurs de synchronisation sans affecter les autres mobiles.
Activer effacement distant	En cliquant sur ce bouton, un message va vous demander de confirmer que vous souhaitez effacer le contenu du mobile. Lorsque l'effacement est initié, son statut apparaît dans la colonne "Effacement distant". **Non supporté** signifie que le mobile n'accepte pas l'effacement distant. **Attente** signifie que la commande sera envoyée à la prochaine synchronisation. Si le mobile ne traite pas le push ou n'est pas connecté, le serveur doit attendre. Après que l'effacement distant ait été exécuté, le mobile est supprimé de la liste et le système envoie un message d'acquittement au propriétaire du compte et à l'administrateur. Le mobile réapparaitra de nouveau dans la liste après la première synchronisation réussie. Note : l'effacement distant est spécifique d'un mobile et non d'un compte. Si un compte a deux mobiles, un effacement distant sur un de ses mobiles n'effacera pas les données sur l'autre.
Désactiver effacement distant	Cliquer sur le bouton pour arrêter l'effacement distant. La désactivation ne peut se faire que dans l'état Attente.
Journaux	Ce bouton ouvre la fenêtre des journaux (Etat -> Journaux -> ActiveSync en introduisant le filtre de l'appareil sélectionné.

Stratégie de sécurité

La stratégie de sécurité permet aux mobiles qui se synchronisent par le protocole ActiveSync sur le serveur IceWarp de protéger leurs données sensibles, que ce soit les emails, les contacts ou des documents stockés sur le mobile. La stratégie de sécurité est appliquée par le serveur avant tout échange de données.

Il est conseillé d'avoir une stratégie de sécurité homogène à travers l'organisation, veiller à ne pas exclure certains mobiles de cette stratégie, à éviter les mobiles non compatibles et à mettre à jour les firmware et OS.

© IceWarp France / DARNIS Informatique

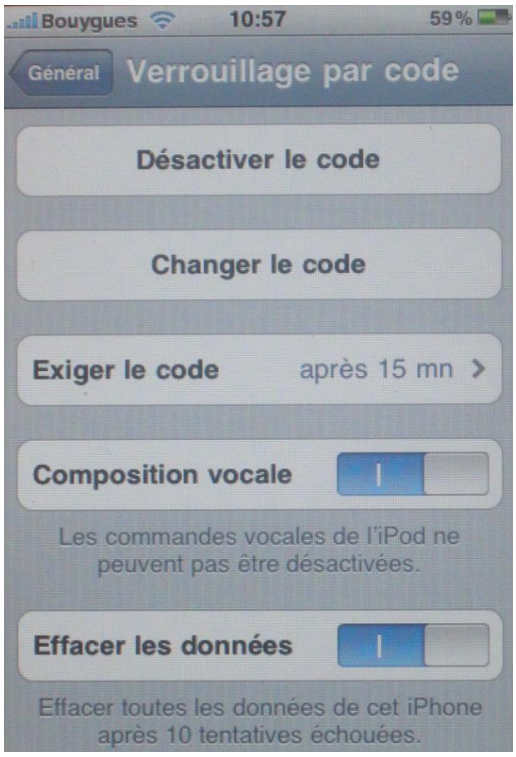
Toute reproduction interdite sans accord d'IceWarp France

Cette stratégie de sécurité couplée avec le mécanisme d'effacement à distance permet d'éviter le vol des données.

Il est d'autre part conseillé d'utiliser les mécanismes locaux de protection comme le verrouillage par code et la validation de l'effacement automatique local du mobile en cas de trop nombreuses tentatives infructueuses de rentrée d'un mot de passe.

Cette stratégie de sécurité n'a aucune incidence sur la durée de la batterie ni sur les performances contrairement à d'autres solutions comme l'encryptage local par exemple.

L'image ci-dessous indique comment configurer les mots de passe sur un iPhone. Ces commandes sont elles-mêmes protégées par le mot de passe (Réglages -> Général -> verrouillage par code).



Effacement local ou distant du mobile

Lorsqu'un mobile est perdu ou volé, il y a un risque potentiel important de compromission des données. Les conséquences peuvent être graves si les données sont sensibles ou confidentielles. ActiveSync permet de limiter ce risque en offrant deux possibilités d'effacement du mobile.

L'effacement d'un mobile localement ou à distance a les mêmes conséquences qu'un reset matériel. L'effacement écrase toutes les données, les configurations et les clés privées du mobile en inscrivant dans la mémoire une séquence de bits qui rend la relecture des données très difficile.

Notes : Le nettoyage des mobiles Windows inclut la carte mémoire externe. Le temps de nettoyage complet d'un iPhone peut atteindre une heure.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Nettoyage local

Le nettoyage local est provoqué sur un mobile ayant l'option d'effacement des données après un certain nombre de tentatives erronées d'entrées du code. Ce nombre peut être modifié par l'utilisateur, il est de 8 en standard.

Après quelques tentatives infructueuses, le mobile affiche un message de confirmation demandant à l'utilisateur de rentrer une chaîne définie (souvent a1b2c3) pour confirmer son action et éviter que l'opération ne soit due à des touches pressées accidentellement.

Dès que le nombre de tentatives erronées est atteint, le mobile efface sa mémoire.

Nettoyage distant

Le nettoyage distant se produit lorsqu'un administrateur lance une commande de nettoyage à travers l'interface de gestion du serveur ActiveSync. Ce nettoyage est indépendant du nettoyage local et ne dépend donc pas de la stratégie de contrôle du mot de passe.

La commande de nettoyage est lancée "hors ligne" ce qui fait que le mobile la recevra à sa prochaine synchronisation. L'utilisateur du mobile ne peut pas empêcher le nettoyage distant.

Confirmation par mail

Le système envoie un message de confirmation dès que le mobile reçoit la commande de nettoyage. Le message alerte le propriétaire du compte et l'administrateur du système.

Restrictions

Les mobiles qui n'ont pas l'option de sécurité, n'autorisent pas le nettoyage distant et le statut de l'effacement distant dans l'interface d'administration indiquera "Non supporté". L'administrateur devra exclure ces mobiles de la stratégie générale de sécurité et inciter leurs utilisateurs à valider le nettoyage local au bout de 10 tentatives erronées.

Définition de la stratégie

L'administrateur peut définir la stratégie de sécurité au niveau global (serveur), domaine, utilisateur et mobile et elle est applicable automatiquement aux utilisateurs individuels.

Il n'y a pas de contraintes de sécurité par défaut.

Stratégies au niveau global

Menu : GroupWare -> ActiveSync -> Gestion des appareils -> Stratégies globales...

La stratégie globale est appliquée à tous les domaines, utilisateurs et mobiles sauf indication contraire à un niveau inférieur.

Par défaut, la sécurité est définie à un niveau "neutre". La sécurité est alors définie librement par chaque utilisateur pour son propre mobile. Les paramètres sont ceux indiqués sur l'écran ci-dessus.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Stratégies au niveau domaine

Menu : Domaines et Comptes -> Gestion -> <domaine> -> onglet Services -> Appareils ActiveSync -> Stratégie des domaines

Les mêmes contraintes de sécurité que ci-dessus peuvent être définies au niveau domaine, soit pour assouplir les contraintes, soit pour les durcir.

Stratégies au niveau Utilisateur

Menu : Domaines et Comptes -> Gestion -> <domaine> -> <Utilisateur> -> onglet Services -> Appareils ActiveSync -> Stratégie des utilisateurs

Les mêmes contraintes de sécurité que précédemment peuvent être définies au niveau utilisateur, soit pour assouplir les contraintes, soit pour les durcir.

Stratégies au niveau appareil

Les sécurités à ce niveau sont particulières puisqu'elles ne peuvent être définies que si le mobile est connecté au serveur (il faut connaître le DeviceID pour le différencier des autres).

L'accès au menu peut se faire par les trois niveaux décrits ci-dessus en sélectionnant l'appareil puis le bouton "Stratégie des appareils..." ou en double cliquant sur l'appareil.

Héritage des stratégies

Les stratégies sont automatiquement héritées lorsque la stratégie du niveau le plus élevé est définie avant celle du niveau inférieur. Si une stratégie de niveau plus élevée a été modifiée et que l'on souhaite la répercuter sur un niveau inférieur, il faut utiliser le bouton "Hériter".

Note : le libellé situé en haut de la boîte de dialogue sur la stratégie de sécurité des appareils indique si les paramètres sont hérités ou sont spécifiques. Dans ce dernier cas, le bouton Hériter est opérationnel (cf. § Références).

Acceptation des stratégies

Une fois la stratégie définie sur le serveur, elle est envoyée vers le mobile à la synchronisation suivante.

A la première réception de la stratégie, l'utilisateur doit l'accepter ou non. Si elle est refusée, l'utilisateur ne pourra pas se synchroniser avec le serveur.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Une fois la stratégie acceptée, le seul moyen de la désactiver est de réinitialiser complètement le mobile par un reset matériel qui va aussi initialiser toutes les données utilisateurs et la configuration.

Si la stratégie change, un message avertissant l'utilisateur est envoyé sur le mobile lui demandant de modifier son mot de passe s'il n'est pas compatible avec la nouvelle stratégie.

Si la stratégie n'est pas acceptée par l'utilisateur ou n'est pas compatible avec le mobile et que la non compatibilité n'est pas acceptée par l'administrateur, un message est envoyé à l'utilisateur et à l'administrateur indiquant que le mobile ne peut se connecter au serveur. Exemple de message envoyé :

Error: Your mobile device (iPhone : Appl85928...) didn't confirm the security profile required by server administrator, therefore cannot connect to the server.

Make sure to accept the security provisioning if prompted, or contact your technical helpdesk for a security exemption.

Exclusion de la politique de sécurité

L'option "Permettre l'accès à un appareil ne supportant pas les contraintes de sécurité" permet d'exclure certains mobiles de la stratégie de sécurité.

Elle permet de spécifier qu'un mobile d'ancienne génération (Windows Mobile 5.0 sans pack additionnel, Palm,...) peut quand même se connecter au serveur alors que les mobiles plus récents bénéficient de toutes les sécurités.

Elle permet aussi d'exclure de la stratégie de sécurité des utilisateurs qui ne souhaitent pas l'appliquer. Cette option est cependant risquée si des données importantes peuvent être synchronisées.

Suppression de la stratégie de sécurité

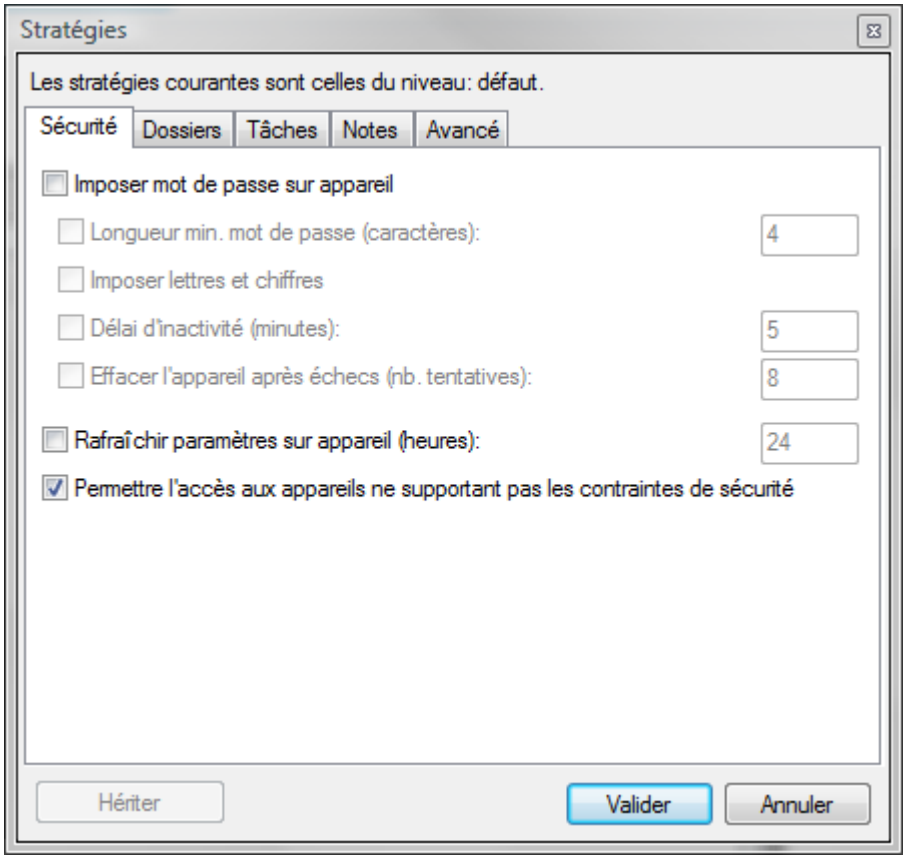
Pour supprimer la stratégie de sécurité sur un mobile particulier, il suffit de sélectionner ce mobile et de décocher l'option "imposer mot de passe sur appareil". Une commande de suppression de la stratégie de sécurité est alors envoyée au mobile et les paramètres par défaut du mobile sont immédiatement pris en compte (si le push est validé).

Note : ceci ne supprime pas le verrouillage par code, il faut une opération manuelle de l'utilisateur pour cela.

Références de la configuration

Voici une description détaillée des différents champs qui sont utilisés pour configurer la stratégie de sécurité.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France



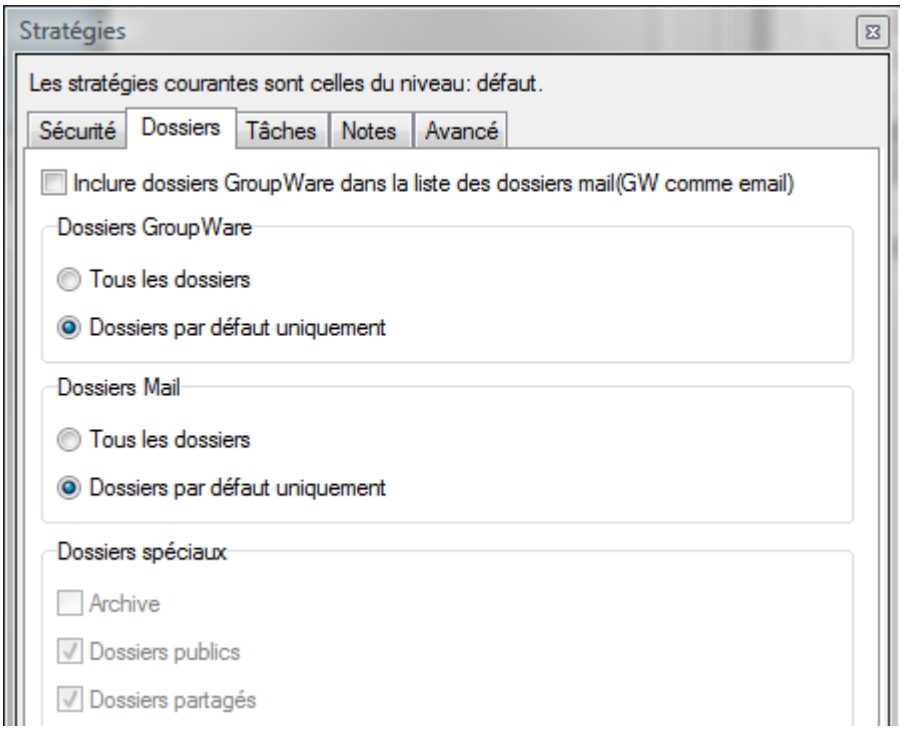
Champ	Description
Libellé en haut de la fenêtre	**"Les stratégies sont héritées du niveau défaut/serveur/domaine/utilisateur"** Ce libellé indique que la stratégie n'a pas été personnalisée à ce niveau et indique de quel niveau elle hérite (niveau le plus haut). **"Pour hériter des stratégies d'un niveau supérieur, cliquez sur le bouton "Hériter" ci-dessous"** Ce libellé indique que le niveau a été personnalisé Note : si le bouton "Hériter" est utilisé à un niveau, les paramètres du niveau juste supérieur sont utilisés. Si les paramètres d'un niveau sont modifiés, tous les niveaux qui en héritent le sont aussi. Ceux qui ont des paramètres spécifiques n'en héritent pas.
Imposer mot de passe sur appareil	Par défaut, les mobiles n'ont pas besoin d'un mot de passe au moment de l'allumage pour pouvoir être utilisés. Si cette option est cochée, un mot de passe sera demandé à la mise sous tension et après un certain délai d'inactivité Si l'option est cochée, les options suivantes deviennent actives et permettent de préciser les conditions d'utilisation du mot de passe.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

	Si cette option n'est pas cochée, l'utilisateur du mobile peut choisir les options de sécurité qu'il désire.
Longueur min mot de passe (caractères)	Si une valeur est indiquée, le mot de passe choisi par l'utilisateur pour son mobile devra s'y conformer sous peine de rejet par le serveur. La longueur peut aller de 2 à 18 caractères. Toute valeur en dehors de cette fourchette sera ramenée à 2 ou 18 automatiquement. Si aucune valeur n'est indiquée, l'utilisateur est libre de choisir son mot de passe comme il veut.
Imposer lettres et chiffres	Si l'option est cochée, le mot de passe doit contenir des chiffres et des lettres (et/ou signes de ponctuation et majuscules). La validité du mot de passe est contrôlée par le mobile. Si l'option n'est pas cochée, l'utilisateur peut choisir le mot de passe qu'il désire.
Délai d'inactivité (minutes)	Si l'option est cochée, il est possible de rentrer la durée d'inactivité au bout de laquelle il sera demandé à l'utilisateur de ré-entrer son mot de passe. Ce délai n'est pas lié au temps d'allumage du mobile qui est limité pour diminuer la consommation. Le délai peut être positionné de 0 à 9999 minutes 0 signifie que le mot de passe sera demandé dès que le mobile est éteint. S'il le mobile n'a pas de temporisation d'extinction, le mot de passe ne sera demandé qu'à la mise en route du mobile.
Effacer l'appareil après échecs (nombre tentatives)	Si l'option est cochée, il est possible de rentrer un nombre de tentatives d'entrée d'un mauvais mot de passe. Au delà de ce nombre, la mémoire du mobile sera effacée. Ce processus est contrôlé par le serveur. Après quelques tentatives infructueuses, le mobile affiche un message de confirmation demandant à l'utilisateur de rentrer une chaîne définie (souvent a1b2c3) pour confirmer son action et éviter que l'opération ne soit due à des touches pressées accidentellement. La valeur du nombre de tentatives est de 0 à 99. Une valeur plus grande sera ramenée à 99. 0 signifie que l'effacement automatique est désactivé et que l'utilisateur ne peut pas l'activer. Si l'option n'est pas cochée, l'option est laissée au libre choix de l'utilisateur du mobile.
Rafraîchir paramètres sur appareil (heures)	Spécifie à quel intervalle la stratégie de sécurité sera synchronisée vers le mobile. Ceci est utile dans le cas de certains utilisateurs qui contournent les options de sécurité qui leur ont été imposées. De cette façon la stratégie de sécurité sera périodiquement réimposée au mobile. Le nombre d'heures pour le rafraîchissement peut être donné de 1 à 9999 heures. Toute valeur supérieure sera ramenée à 9999.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

	Si l'option n'est pas cochée, la stratégie sera appliquée une seule fois. A la première synchronisation après création du compte sur le mobile ou à la prochaine synchronisation si le compte existe déjà.
Permettre l'accès à un appareil ne supportant pas les contraintes de sécurité	Si la case est cochée, cela signifie que tous les mobiles peuvent se synchroniser avec le serveur. Aussi bien les mobiles qui ne supportent pas les stratégies de sécurité que ceux dont l'utilisateur l'a refusée. C'est l'option par défaut. Si la case n'est pas cochée, les mobiles qui ne supportent pas la stratégie de sécurité reçoivent un message d'erreur de type "449 Needs provisioning" et ne peuvent se synchroniser. L'utilisateur et l'administrateur reçoivent alors un message d'erreur.
Hériter	Cliquer pour hériter du niveau supérieur. Pour plus de détails voir l'explication sur la deuxième ligne de ce même tableau
Valider	Après avoir cliqué sur Valider, la configuration est sauvegardée.
Annuler	Pour quitter la fenêtre sans appliquer les modifications.

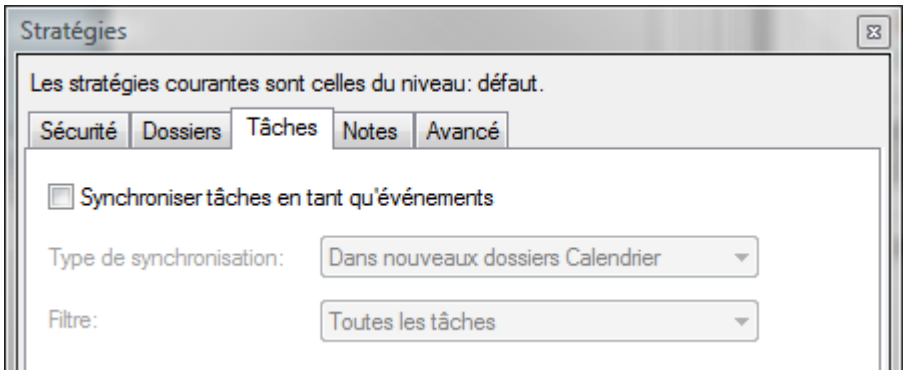


Champ	Description
Inclure dossiers GroupWare dans la liste des dossiers mail	Certains clients ActiveSync ne supportent pas la gestion des dossiers, les arborescences de dossiers ou certains types de dossiers. En cochant cette case, les documents apparaîtront dans la liste des emails.

© IceWarp France / DARNIS Informatique

Toute reproduction interdite sans accord d'IceWarp France

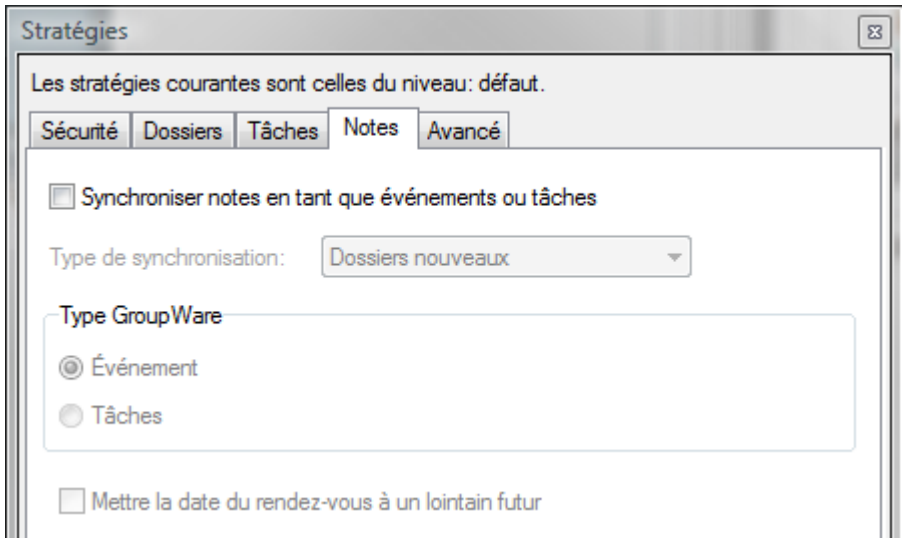
(GW comme email)	
Dossiers GroupWare	
Tous les dossiers	Si vous voulez voir tous les dossiers GroupWare du compte
Dossiers par défaut uniquement	Pour ne voir que le dossier par défaut de chaque type : calendrier, contacts, tâches...
Dossiers Mail	
Tous les dossiers	Si vous voulez voir tous les dossiers mail du compte
Dossiers par défaut uniquement	Pour ne voir que le dossier par défaut : inbox, envoyés, corbeille....
Dossiers Spéciaux	
Archives	pour synchroniser le dossier archives vers le mobile
Dossiers publics	pour synchroniser les dossiers publics vers le mobile
Dossiers partagés	pour synchroniser les dossiers partagés vers le mobile



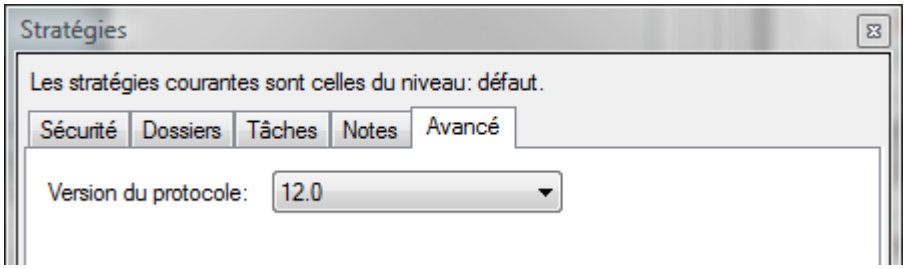
Champ	Description
Synchroniser tâches en tant qu'événement	Permet de voir les tâches sur les mobiles qui ne synchronisent pas les tâches directement. Cela n'influence pas les mobiles qui synchronisent les tâches.
Type de synchronisation	*Dans nouveaux dossier calendriers* : les tâches sont crées dans un nouveau dossier. Il peut arriver que le dossier soit dupliqué. *Fusionner avec le calendrier par défaut* : à sélectionner pour les mobiles qui ne synchronisent que le dossier par défaut.
Filtre	*Toutes les tâches* : toutes les tâches sont synchronisées

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

	Tâches inachevées uniquement : seules les tâches non terminées sont synchronisées



Champ	**Description**
Synchroniser en tant qu'événement ou tâches	Permet de voir les notes sur les mobiles qui ne synchronisent pas les notes directement. Cela n'influence pas les mobiles qui synchronisent les notes.
Type de synchronisation	*Dossiers nouveaux* : les notes sont crées dans un nouveau dossier. Il peut arriver que le dossier soit dupliqué. *Fusionner avec dossier par défaut* : à sélectionner pour les mobiles qui ne synchronisent que le dossier par défaut.
Type de GroupWare	*Evénement* : la note est synchronisée comme un événement. A sélectionner si le mobile ne supporte pas les tâches *Tâches* : à sélectionner de préférence si le mobile synchronise les tâches car les notes sont plus proches d'une tâche que d'un événement



© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Champ	Description
Version du protocole	Sélectionner la plus haute version supportée. les versions précédentes sont aussi supportées. 12.0 est la version recommandée. 12.1 et 14 sont aussi supportées mais pas complètement testées.

SSL et les mobiles Windows

Exigences SSL

Le push direct et la découverte intelligente ne fonctionnent correctement sur les mobiles Windows que si SSL est validé lorsque le compte ActiveSync est configuré. En plus, le certificat SSL fourni par le serveur doit être préalablement approuvé par le mobile car l'approbation ne sera pas demandée à l'utilisateur et la connexion SSL ne sera donc pas établie. Un certificat SSL peut être approuvé selon une de ces méthodes :

1. Méthode recommandée : obtenir un certificat certifié par une autorité de certification qui est déjà reconnue par le mobile (voir ci-dessous les certificats reconnus par les mobiles Windows ou aller dans Settings -> System -> Certificates -> root sur le mobile). Installer ce certificat sur le serveur. Pour plus de détails voir l'aide en ligne de la console d'administration sur Système -> Certificats.

2. Méthode non recommandée : obtenir un certificat pour le serveur signé par une autorité intermédiaire. Cela signifie que vous devez installer le certificat intermédiaire sur tous les mobiles.

3. Méthode réservée pour des tests ou des utilisations spéciales : Utilisez votre certificat auto signé et importez le certificat dans le répertoire des certificats racines de tous les mobiles.

Windows Mobile 5.0 et Windows Mobile 6.x

Avec la méthode 1, il n'y a rien à faire sur le mobile. Pour les méthodes 2 et 3, il faut installer un certificat sur le mobile, procéder de la façon suivante :

1. Exporter le certificat racine avec les utilitaires SSL au format binaire X509 avec une extension .cer.

2. Copier le certificat dans le répertoire \Storage du mobile ou sur le dossier root d'une carte mémoire en utilisant une connexion câblée via l'application desktop ActiveSync (Tools -> Explore).

3. Ou envoyez-vous le certificat par mail par un compte POP/IMAP que vous avez configuré avant le compte activeSync puis le télécharger de la boîte de réception.

4. Recherchez finalement le fichier sur le mobile en utilisant l'explorateur de fichier, double cliquez sur le fichier et confirmez que vous voulez l'importer sur le mobile.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

5. Pour vérifier que le certificat a bien été installé, appuyez sur Start, sélectionnez Settings puis l'onglet System -> Certificates. Le certificat doit apparaître soit sur l'onglet intermédiaire, soit sur l'onglet racine.

Note : la possibilité d'installer un certificat dépend de la façon dans le mobile a été configuré par l'équipementier (OEM) ou par l'opérateur mobile.

Pocket PC / Smartphones 2002 et 2003

Ces mobiles ne supportent pas le push direct ni la découverte intelligente mais vous pouvez quand même avoir envie d'utiliser des connexions SSL. PocketPC 2002 et 2003 ne se connectent qu'à travers SSL. Les mobiles ayant Windows Mobile 2003 n'ont pas besoin de SSL. Il est cependant fortement recommandé d'utiliser SSL pour protéger vos données qui, sinon, sont transmises en clair puisque c'est la seule possibilité offerte par l'architecture EAS.

Ces mobiles utilisent Microsoft Crypto API (CAPI) pour stocker de façon sûre les certificats racine et il peut être nécessaire d'importer un outil Microsoft spécifique pour les importer.

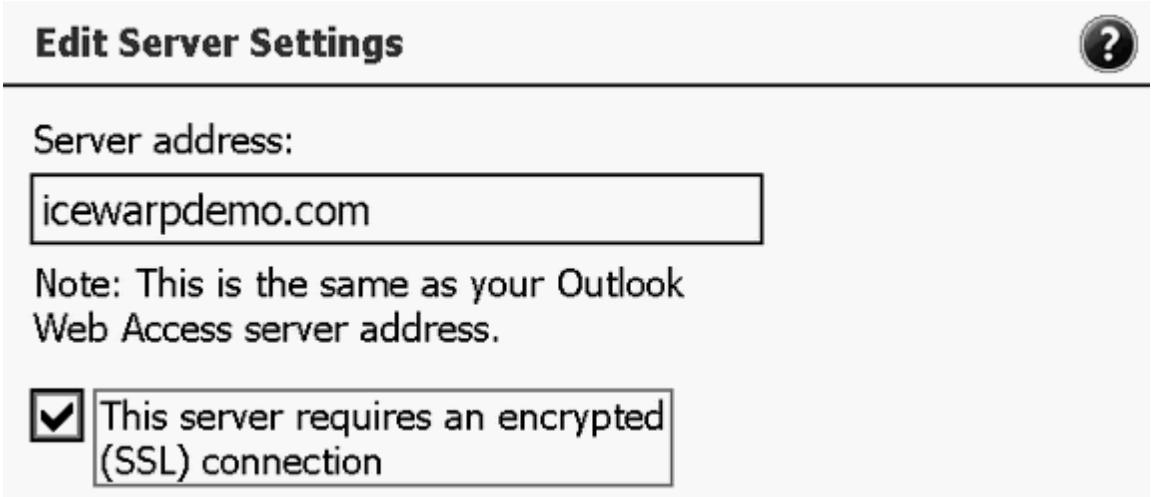
Pour plus de détails sur cette procédure, voir le lien :

http://support.microsoft.com/?id=841060

Note : l'opérateur qui a fourni le mobile peut avoir restreint les possibilités d'importation de certificats racines.

Valider SSL pour ActiveSync

Pour valider l'authentification SSL sur les mobiles Windows 2003/5.0/6.0/6.1 (et donc le push direct et la découverte intelligente), il faut aller dans la configuration du serveur de synchronisation ActiveSync et sélectionner l'option "This server requires an encrypted (SSL) connection" :



© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Certificats de confiance pour Windows Mobile

Pour simplifier le déploiement et permettre un accès sécurisé à tous les services du serveur IceWarp, nous recommandons instamment l'installation sur le serveur d'un certificat émanant d'une autorité de certification reconnue par les mobiles. Comme alternative, il est possible d'installer un certificat émanant d'une société reconnue par une autorité que le mobile reconnaît. Les certificats SSL de sociétés connues sont signés par une autorité de certification qui est présente dans le dossier des certificats racines des mobiles.

Si vous déployez différents mobiles, sélectionnez l'autorité de certification présente dans le mobile dont l'OS est le plus ancien.

Les certificats racines contenus dans les mobiles PocketPC 2002 émanent des autorités suivantes :

- VeriSign
- Cybertrust
- Thawte
- Entrust

Les certificats racines contenus dans les mobiles PocketPC 2003 émanent des autorités suivantes :

- VeriSign
- Cybertrust
- Thawte
- Entrust
- GlobalSign
- Equifax

Les certificats racines contenus dans les mobiles Windows Mobile 5.0 émanent des autorités suivantes:

- Class 2 Public Primary Certification Authority (VeriSign, Inc.)
- Class 3 Public Primary Certification Authority (VeriSign, Inc.)
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- Equifax Secure Certification Authority
- GlobalSign Root CA
- GTE CyberTrust Global Root
- GTE CyberTrust Root

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

- Secure Server Certification Authority (RSA)
- Thawte Premium Server CA
- Thawte Server CA

Les Windows Mobile 5.0 avec AKU2(MSFP) ont le certificat racine supplémentaire suivant :

- Godaddy http://www.valicert.com/

Les certificats racines contenus dans les mobiles Windows Mobile 6.x émanent des autorités suivantes:

- Comodo AAA Certificate Services
- Comodo AddTrust External CA Root
- Cybertrust Baltimore CyberTrust Root
- Cybertrust GlobalSign Root CA
- Cybertrust GTE CyberTrust Global Root
- Verisign Class 2 Public Primary Certification Authority
- Verisign Thawte Premium Server CA
- Verisign Thawte Server CA
- Verisign Secure Server Certification Authority
- Verisign Class 3 Public Primary Certification Authority
- Entrust Entrust.net Certification Authority (2048)
- Entrust Entrust.net Secure Server Certification Authority
- Geotrust Equifax Secure Certificate Authority
- Geotrust GeoTrust Global CA
- Godaddy Go Daddy Class 2 Certification Authority
- Godaddy http://www.valicert.com/
- Godaddy Starfield Class 2 Certification Authority

Détails techniques

Pour plus d'informations sur les certificats avec Windows mobile, consultez cet article :

http://technet.microsoft.com/en-us/library/cc182301.aspx

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Configuration du mobile

Attention : la première synchronisation va supprimer toutes les données déjà présentes dans le mobile (contacts, calendriers, mails...) et les remplacer par celles du compte sur le serveur. Ceci est le comportement nominal lorsqu'un mobile est nouvellement associé à un compte du serveur ; il permet d'éviter la duplication.

Sauvegarde des données

Si le mobile contient des données importantes (contacts et calendrier) qu'il faut préserver, certains mobiles peuvent le faire. Il faut utiliser une procédure de synchronisation bidirectionnelle :

A titre individuel, faites une sauvegarde de vos données en utilisant les outils spécifiques fournis avec votre mobile (ActiveSync, iSync, Nokia PC suite). Vous pourrez ensuite restaurer ces données sur le mobile qui les synchronisera avec le compte serveur.

En production, vous avez deux possibilités :

- soit déplacer les contacts sur une carte SIM puis après la synchronisation par ActiveSync, les copier dans le carnet d'adresses

- soit effectuer une synchronisation par SyncML au préalable pour synchroniser les données vers le serveur (synchronisation bi ou mono directionnelle). Les mêmes données seront alors disponibles, après la première synchronisation ActiveSync, les données seront disponibles à la fois sur le mobile et sur le serveur.

Configuration

Recherchez le menu de configuration **d'ActiveSync** sur le mobile. Généralement, lorsque vous créez un compte, un assistant vous guide dans le processus de configuration. Si un compte ActiveSync existe déjà, il faut d'abord le supprimer (ce qui supprime toutes les données associées). Les informations nécessaires à la synchronisation du mobile avec le serveur sont les suivantes :

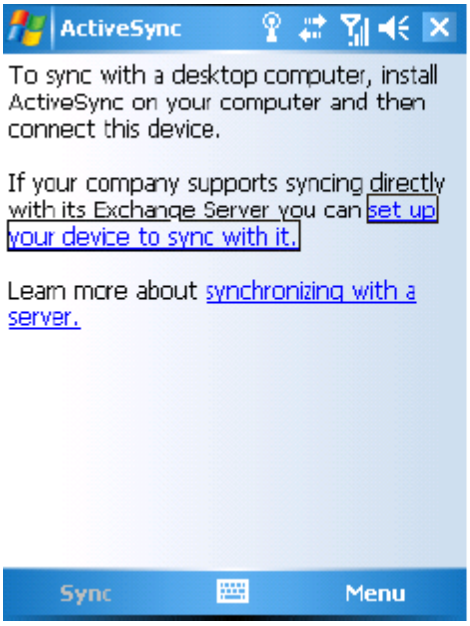
- **Le nom d'utilisateur** : c'est l'adresse mail complète de l'utilisateur (<alias>@<nom de domaine>)
- **Le mot de passe** : le mot de passe de l'utilisateur (le même que pour la connexion au client Web)
- **Le nom de domaine** est parfois demandé mais il est facultatif
- **Le nom du serveur** : si la découverte intelligente ne fonctionne pas, il faut donner le nom du serveur IceWarp : ce peut être une adresse IP ou le nom connu par le réseau (à demander à votre administrateur - par exemple : comserver.darnis.com)

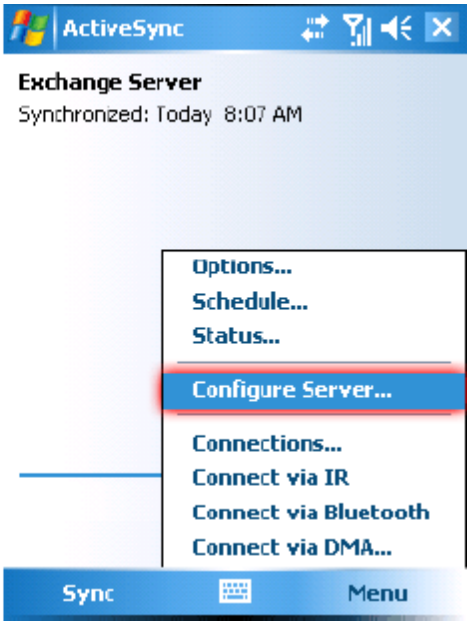
© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Choix du mode de synchronisation ActiveSync

Mobiles Windows

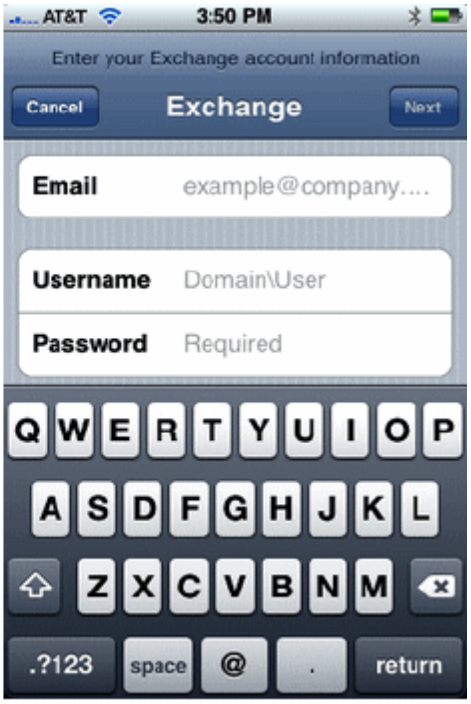
Démarrage -> Programmes -> ActiveSync -> Menu -> Ajouter un serveur source





iPhone

Réglages -> Mail, Contacts, Calendrier -> Ajouter un compte... -> Microsoft Exchange



© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

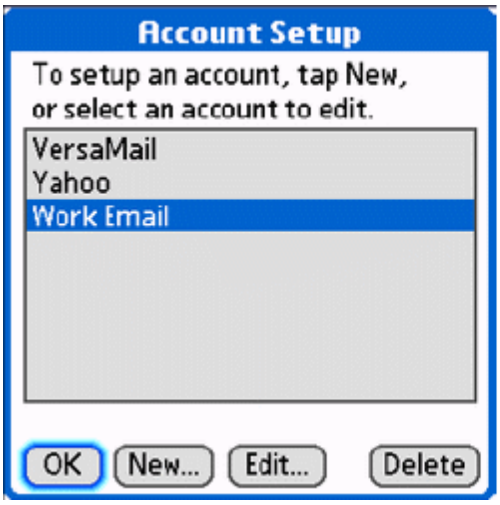
Nokia (Symbian S 60)

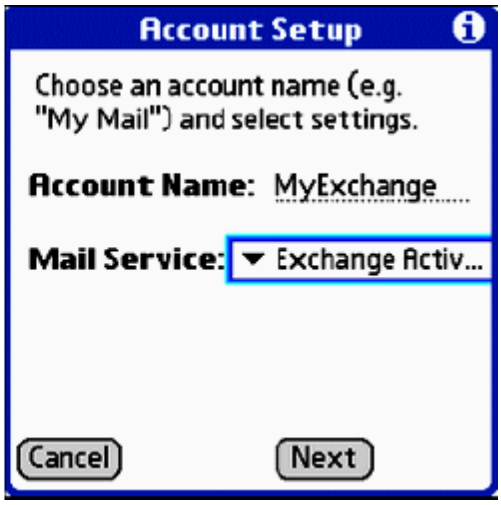
Aller dans Menu -> installations -> Mail For Exchange (module à installer s'il ne l'est pas).

Tous les éléments de configuration sont alors disponibles dans le menu options.

Palm OS

Menu -> Messagerie -> Comptes -> configuration d'un compte... -> Nouveau -> Type de messagerie : Outlook (EAS)





© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Palm Pré

Démarrage rapide -> Mails -> (Préférences et comptes, Ajouter un compte si besoin) -> entrez l'adresse mail et le mot de passe -> Changez l'option du type de messagerie en Exchange (EAS).

Symbian UIQ

Menu -> Applications -> RoadSync -> Options -> Configurations

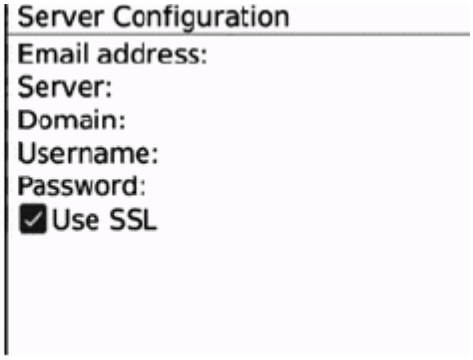
Quand vous installez l'application client sur le mobile, un assistant vous guide à travers le processus de configuration. Pour plus de détails, voir la documentation qui accompagne le produit.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

BlackBerry

Applications -> AstraSync/NotifySync -> Options

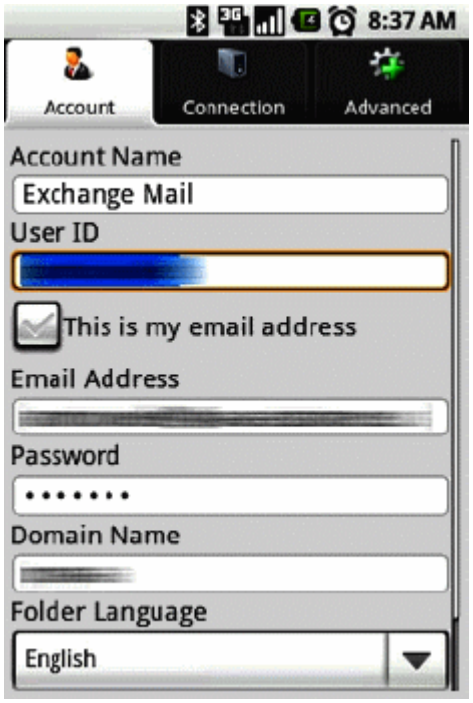
Quand vous installez l'application client sur le mobile, un assistant vous guide à travers le processus de configuration. Pour plus de détails, voir la documentation qui accompagne le produit.



Android (TouchDown)

Menu -> Applications -> TouchDown -> Configuration -> Comptes

Quand vous installez l'application client sur le mobile, un assistant vous guide à travers le processus de configuration. Pour plus de détails, voir la documentation qui accompagne le produit.

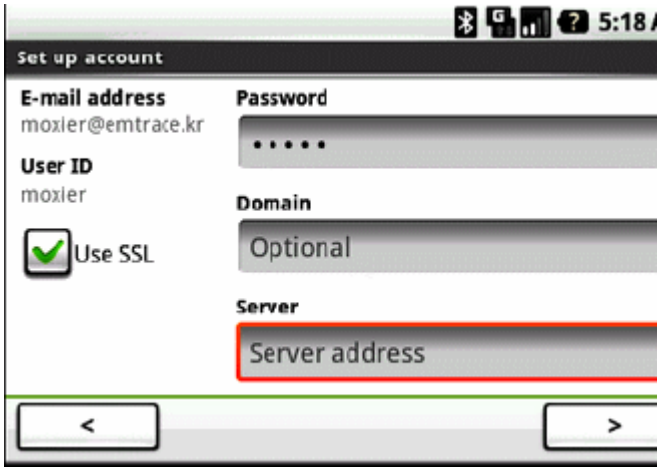


© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Android (Moxier Mail)

Menu -> Applications -> Moxier Sync -> Comptes

Quand vous installez l'application client sur le mobile, un assistant vous guide à travers le processus de configuration. Pour plus de détails, voir la documentation qui accompagne le produit.



Configuration du compte

Pour les mobiles qui utilisent la **découverte intelligente**, il faudra rentrer l'adresse mail et le mot de passe ; le nom du serveur et le nom de domaine sont retrouvés automatiquement grâce au nom de domaine de l'adresse mail (directement grâce au nom si le nom du serveur contient le domaine ou par recherche d'un enregistrement MX du DNS sinon).

- Nom d'utilisateur : adresse complète de l'utilisateur

- Mot de passe

Il vous sera peut-être demandé d'accepter un certificat SSL non authentifié s'il n'y a pas de certificat déjà installé et si le serveur utilise un certificat auto signé plutôt qu'un certificat signé par une autorité de confiance.

Pour les mobiles qui n'utilisent pas la découverte intelligente il faudra aussi fournir :

- Le nom du serveur

- Le domaine : cette information est facultative, elle peut être laissée vide.

Note : ne pas utiliser http:// ou https:// dans le nom du serveur ni de / à la fin

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Autres éléments de configuration

Il y a en général une option qui permet de valider la synchronisation des messages, contacts et calendrier.

Dans les options supplémentaires on peut trouver:

- Validation du push ou synchronisation à période fixe
- Définition de la plage de données à synchroniser (mails et calendrier)
- Le choix des dossiers pour la synchronisation avec les applications embarquées
- Tout autre paramètre de configuration spécifique du mobile utilisé et des applications embarquées.

Les mots de passe sont transmis en clair par le protocole ActiveSync, il est donc vivement recommandé de valider **l'option SSL** (obligatoire sur l'iPhone) qui crypte toute la communication.

Note : il est conseillé de limiter la plage des messages synchronisés à un nombre limité de jours. Les durées de synchronisation et la consommation de la batterie seront largement limitées si une erreur se produit e qu'une resynchronisation complète s'avère nécessaire.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Problèmes de fonctionnement

En cas de problème de fonctionnement

Version d'IceWarp

Avez-vous bien effectué la mise à jour de votre version 9 vers la version 10 directement sur le serveur ? Autrement dit, êtes vous certain de n'avoir pas restauré la configuration de la version 9 sur la version 10 ?

Les paramètres de configuration qui sont sauvegardés ne sont pas compatibles entre la version 9 et la version 10, donc, si vous avez restauré une configuration de la v9 sur la v10, le fichier webservice.dat risque d'être corrompu et plusieurs services risquent de ne pas fonctionner. Voir plus loin pour une éventuelle correction de ce fichier.

Pendant l'installation d'une v10 sur une v9 il y a plus de 40 scripts qui s'exécutent touchant particulièrement la base de données GroupWare ; il est donc tout à fait déconseillé de ne pas exécuter la procédure normale.

Configuration du serveur

Vérifiez que vous avez correctement exécuté la configuration serveur telle que décrite précédemment

Configuration du mobile

Vérifiez que vous avez correctement exécuté la configuration du mobile telle que décrite précédemment

Vérifiez les messages d'erreurs

Échec d'authentification - revérifiez le nom d'utilisateur et le mot de passe sur le mobile. Le nom d'utilisateur est toujours une adresse mail complète.

Échec de connexion au serveur - Vérifiez votre connexion sans fil. Certains mobiles sont prévus pour utiliser une connexion WiFi ce qui ne marche pas avec ActiveSync sur Http. Il faut souscrire à un abonnement GPRS/3G avec accès Internet.
Vérifiez le nom d'hôte dans la configuration ActiveSync.
Vérifiez que vous pouvez vous connecter au Client Web à partir du navigateur du mobile (en ajoutant /webmail/pda au nom du serveur).
Vérifiez que votre serveur Web tourne sur les ports standards (80 et 443 pour le port sécurisé).
Vérifiez que vous avez une règle de réécriture dans la configuration des services Web.
Vérifiez dans la configuration des services Web que l'onglet Documents comprend index.php.

Généralement, après avoir authentifié le compte, le mobile va faire apparaître un "Avertissement sur le certificat SSL" dans le cas d'un certificat auto signé sur le serveur et lorsque le mobile se connecte au service de découverte automatique. Si le service n'est pas trouvé ce message va apparaître plus tard après que vous ayez rentré le nom du serveur. Si ce n'est pas le cas, le problème n'est pas dans ActiveSync mais plutôt dans la configuration du serveur ou du réseau.

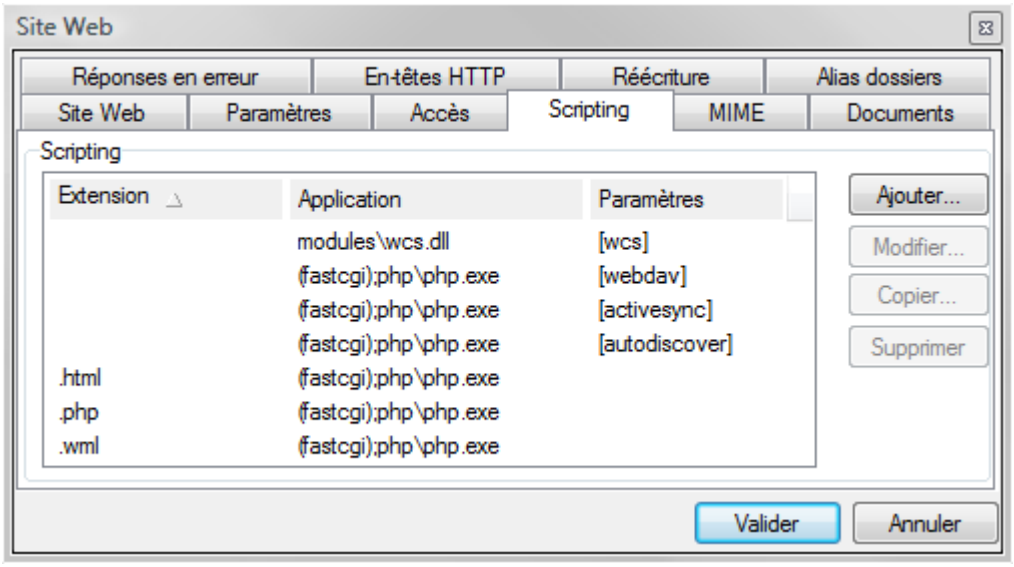
© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Pour vérifier que la connexion au service Web fonctionne, utilisez un navigateur et essayez la connexion suivante au serveur :

```
https://nom d'hôte/Microsoft-Server-ActiveSync/
```

Une fenêtre doit s'ouvrir pour demander le nom d'utilisateur et le mot de passe. Si ce n'est pas le cas c'est que le service Web n'est pas bien configuré, les paramètres de Scripting pour ActiveSync manquent, un pare-feu bloque la connexion ou il y a une autre erreur réseau.

Vérifiez la configuration de l'onglet Scripting du Serveur Web (le serveur par défaut en général). Il devrait ressembler à la copie d'écran ci-dessous. Les entrées correspondantes sont dans ...\config\webserver.dat.



Notez qu'il doit y avoir une entrée ActiveSync dans le groupe <Extensions> et dans le groupe <special> :

```
<EXTENSIONS>
        <ITEM>
            <TITLE>[activesync]</TITLE>
            <EXT/>
            <MODULE>php\php.dll</MODULE>
         </ITEM>
      </EXTENSIONS>
      <SPECIAL>
         <ITEM>
            <TITLE>/microsoft-server-activesync</TITLE>
            <MODULE>[activesync]</MODULE>
            <SCRIPT>activesync\index.html</SCRIPT>
         </ITEM>
      </SPECIAL>
```

Autres messages d'erreur - Regarder le message en détail et consultez l'aide en ligne.
Faites un reset matériel de votre mobile.
Désactivez puis réactivez la synchronisation des éléments qui posent problème.
Supprimez le compte de l'utilisateur ActiveSync sur le mobile puis recréez-le.
Utilisez l'option ActiveSync -> effacement du mobile pour redémarrer une synchronisation complète.
Téléchargez les dernières versions des logiciels du mobile et de l'application utilisée.
Consultez le manuel de l'utilisateur du mobile ou contactez l'aide en ligne du fournisseur du mobile ou de l'application.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Pour les mobiles Windows il y a une liste de tous les codes d'erreurs sur le Web. La description textuelle peut aussi être utile pour les autres mobiles utilisant ActiveSync mais il faut cependant noter que beaucoup d'informations sont spécifiques de Microsoft Exchange et ne sont donc pas directement applicables :

`http://www.pocketpcfaq.com/faqs/activesync/exchange_errors.php`

Pas de message d'erreur mais pas de synchronisation non plus - Passez en revue toutes les raisons mentionnées ci-dessus.

Si aucune ne s'applique cela signifie que la base de données a été incorrectement migrée. Cela a pu se produire après une mise à jour d'une version plus ancienne d'IceWarp provoquant un codage incorrect des noms de dossiers en UTF-8. Pour vérifier, essayez une synchronisation avec un nouveau compte. Si ça marche, il va falloir corriger des enregistrements de la base de données GroupWare.
Premièrement, faites une sauvegarde complète de la base de données pour un retour en arrière si besoin. Puis dans la console d'administrations -> Système -> Outils -> migration base de données , sélectionnez la base de destination et cliquez sur "Réparer les caractères UTF-8".
Démarrez la migration. Une fois terminée allez dans GroupWare -> Général -> onglet Général et dans paramètres BD, sélectionnez la base que vous venez de créer.
Validez les modifications et redémarrez le service GroupWare.

En cas de persistance du problème, contactez le support (support@icewarp.fr).

Journal ActiveSync et réinstallation

Validez le journal ActiveSync (Système -> Journaux -> Services) puis analysez l'activité du compte en question à travers ce journal.

S'il n'y a pas d'entrées dans le journal, le service ne s'est pas initialisé.
Cela peut être dû à une mauvaise configuration du processus PHP.
Consultez le journal des erreurs PHP. Réinstallez le serveur IceWarp pour corriger un problème d'installation de PHP.
Vous pouvez aussi réinstallez le serveur IceWarp pour corriger un problème d'installation de ActiveSync.

Si malgré cela il y a encore des erreurs dans le journal que vous ne comprenez pas, envoyez-le à votre service support en indiquant de quel compte il s'agit et en précisant les principales caractéristiques du mobile et du serveur IceWarp.

Fonctionnement aléatoire du Push

Le Push fonctionne de temps en temps, s'arrête, repart...
Vérifiez qu'il n'a y pas un paramètre de planification susceptible d'arrêter le Push.
Si vous utilisez seulement le WiFi assurez vous qu'il n'y a pas un paramétrage qui bloque le WiFi lorsque l'écran est éteint ou le mobile en veille ou bloqué.

Sur le mobile, désactivez tout élément de configuration qui pourrait toucher la période de pulsation du mobile ou mettez la à une valeur plus faible (la maximum accepté par le serveur est de 30 minutes, voir le chapitre sur le changement de la période de pulsation).
La période de pulsation est la durée qui sépare l'envoie de deux "pings" vers le serveur. Regardez les journaux de ActiveSync pour savoir au bout de combien de temps le mobile se déconnecte et s'il se reconnecte ou non. Dans certains cas, un point d'accès WiFi mal configuré peut empêcher le mobile de se reconnecter. Essayez un autre réseau ou coupez le WiFi pour savoir si le problème est lié uniquement au WiFi ou à la connexion WiFi + 2G/3G.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Vérifiez les paramètres de sauvegarde de la batterie. Certains modèles (tel que les Nokia de la série E) coupent la connexion automatiquement lorsque le niveau batterie est faible. Le BlackBerry coupe complètement la radio sur batterie basse.
Après chargement de la batterie, la reconnexion du mobile peut durer plus d'une période de pulsation ce qui peut conduire à la perte d'événements. Dans un tel cas il vaut mieux utiliser la commande "synchroniser tout de suite" pour rétablir la connexion.

Le Push ne fonctionne pas

La fonction Push n'est peut-être pas disponible (PocketPC, Windows Mobile 5.0), vérifiez pour cela la matrice de compatibilité d'ActiveSync.

Tous les mobiles Windows et certains Nokia nécessitent SSL pour que le Push fonctionne. Voir le chapitre sur SSL et les mobiles Windows. Le certificat SSL peut aussi avoir expiré.

Sur le mobile, assurez-vous que le Push est validé. Sur les mobiles Windows, aller dans ActiveSync -> Menu -> Schedule -> Peak times/Off peak times et sélectionnez "As time arrive".
Sur les iPhones, allez dans Réglages -> Mails, contacts, Calendriers -> Nouvelles données et validez le Push.
Sur les autres mobiles, des options de même type existent aussi.

Les mobiles Windows ne permettent pas le Push si le WiFi est la seule liaison disponible. Même si le push est validé, ils vont contacter le serveur toutes les 30 minutes pour détecter les changements jusqu'à l'établissement d'une liaison cellulaire (GPRS, EDGE, 3G).

La plupart des mobiles coupent les connexions de données à l'étranger (roaming), réactiver cette option si besoin.

Certains mobiles permettent de définir une plage horaire pour le push. Vérifiez que cette plage correspond à vos besoins.

Sur le serveur IceWarp, vérifiez que le serveur Push est actif dans GroupWare -> Général -> onglet Serveur Push.

Validez le journal du Push (Système -> Journaux -> Services -> Push GroupWare). S'il reste vide pendant un certain temps alors qu'il y a suffisamment d'activité sur les messages et le GroupWare du serveur, redémarrez le service Contrôle.

Souvenez-vous : pas de Ping, pas de Push ! Le mobile doit envoyer un Ping au serveur pour que celui-ci renvoie un Push. Recherchez dans le journal les entrées "<<< Ping" associées avec le compte ou le mobile en cause.

Une entrée du journal ActiveSync lorsque de nouvelles données doivent être envoyées, doit ressembler à :

```
ebd2dde8d9694f20063f8d9c836c73ea [lab@laberverie] [0000] 13:37:46 <<< Ping
 <Ping xmlns="Ping:">
   <HeartbeatInterval>1020</HeartbeatInterval>
 </Ping>

ebd2dde8d9694f20063f8d9c836c73ea [lab@laberverie] [0000] 13:37:47 >>> 200 OK
 <Ping xmlns="Ping:">
   <Status>2</Status>
   <Folders>
     <Folder>af1cd994dfcb9286c394d142687ff5a0</Folder>
   </Folders>
 </Ping>

ebd2dde8d9694f20063f8d9c836c73ea [lab@laberverie] [0000] 13:37:50 <<< Sync
 <Sync xmlns="AirSync:">
```

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

```
   <Collections>
     <Collection>
       <Class>Email</Class>
       <SyncKey>170</SyncKey>
       <CollectionId>af1cd994dfcb9286c394d142687ff5a0</CollectionId>
       <DeletesAsMoves/>
       <GetChanges/>
       <WindowSize>50</WindowSize>
       <Options>
         <FilterType>2</FilterType>
         <Truncation>1</Truncation>
         <MIMETruncation>1</MIMETruncation>
         <MIMESupport>0</MIMESupport>
       </Options>
     </Collection>
   </Collections>
 </Sync>

ebd2dde8d9694f20063f8d9c836c73ea [lab@laberverie] [0000] 13:37:50 >>> 200 OK
 <Sync xmlns="AirSync:">
   <Collections>
     <Collection>
       <Class>Email</Class>
       <SyncKey>171</SyncKey>
       <CollectionId>af1cd994dfcb9286c394d142687ff5a0</CollectionId>
       <Status>1</Status>
       <Commands>
         <Add>
           <ServerId>4673</ServerId>
           <ApplicationData>
             ...
           </ApplicationData>
         </Add>
       </Commands>
     </Collection>
   </Collections>
 </Sync>

ebd2dde8d9694f20063f8d9c836c73ea [lab@laberverie] [0000] 13:38:03 <<< Ping
```

Note 1 : dans certains cas, il y a des signes non valides en HTML comme par exemple les < et > qui apparaissent dans les adresses de messageries et qui devraient être remplacés par les ensembles < et >. Dans les journaux, ces signes ne sont pas remplacés pour faciliter la lisibilité.

Note 2 : La commande Ping émise par le mobile est émise toutes le X minutes (où X est la période de pulsation, cette période peut aller sur le serveur de 1 à 30 minutes - si le réglage du mobile est de 60 minutes, il sera donc ramené à 30 par le serveur) de façon à indiquer au serveur que le mobile attend les changements sur l'adresse IP de l'expéditeur et pour conserver la session en cours. Le serveur envoie une réponse au mobile pendant cet intervalle dès qu'un changement se produit sur les données du serveur et une synchronisation de ces données est alors initialisée. Une fois la synchronisation terminée, un nouveau Ping est immédiatement envoyé indépendamment de la période de pulsation.

Note 3 : Le mobile peut changer la période de pulsation en fonction de la configuration ou de la charge de la batterie.

Réinitialiser la base de données ActiveSync

Attention : cette opération entraine la synchronisation complète de certains mobiles ce qui peut provoquer l'arrêt du fonctionnement du Push pendant plus d'une heure.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Une synchronisation complète signifie que toutes les données synchronisables du mobile seront supprimées puis resynchronisées. Ceci peut provoquer des transferts de données très importants et une forte consommation de la batterie. Il est par conséquent recommandé de toujours limiter l'ancienneté des messages synchronisés.

ActiveSync utilise une base de données pour les données qui sont synchronisées mais qui doivent être sauvegardées quand un service ou le serveur est redémarré. Aucune intervention n'est nécessaire directement sur cette base de données, les entrées de la base sont gérables à partir de la console d'administration dans Domaines et Comptes -> Gestion -> <utilisateur> -> Services -> Appareils ActiveSync ; il est possible de voir les mobiles actifs, désactiver le compte, enlever un mobile obsolète, faire un nettoyage à distance et régler la stratégie de sécurité.

La base de données est préconfigurée à l'installation du serveur et utilise une connexion PDO. Par défaut, elle utilise SQLite RDBMS (comme le Client Web) qui est installé par défaut avec PHP ; pour de meilleures performances, il est possible d'utiliser MySQL ou MS SQL en allant sur Client Web -> onglet Général -> connexion PDO.

Pour résoudre des problèmes de fonctionnement avec ActiveSync, vous pouvez avoir besoin de supprimer la base de données (ou juste la renommer pour garder une sécurité) :

Supprimer le fichier ...\calendar\activesync\db\sync.db

Aucune donnée ne sera perdue (elles sont stockées indépendamment dans la base de données GroupWare), la liste des mobiles sera simplement vidée et remplie à nouveau au fur et à mesure de leurs connexions.

Pour résoudre des problèmes de connexion sur un compte particulier, l'administrateur utilisera de préférence l'option suivante : ActiveSync -> Gestion des appareils -> Supprimer appareil pour le même résultat mais seul cet appareil sera réinitialisé et soumis à une resynchronisation complète.

Changer la période de pulsation

Dans certains cas assez rare, vous voudrez essayer de modifier la période de pulsation du Push. Le serveur IceWarp accepte toute période de pulsation demandé par le mobile inférieure à 30 minutes. Normalement, le mobile configure automatiquement une période optimale pour la pulsation. Il est possible de la régler manuellement sur certains mobiles. L'augmenter peut sauvegarder la batterie mais une durée supérieure à 30 minutes n'est pas recommandée car ces sessions peuvent être interrompues par les routeurs. La diminuer garantie une mise à jour plus fréquente de l'adresse IP d'écoute du mobile ce qui peut être utile si le Push s'arrête assez régulièrement après un certain temps.

Il est possible de modifier la valeur maximum acceptée par le serveur à l'aide d'une commande en ligne (outil Tool) :

Pour voir la valeur courante (en milli secondes) :

```
tool display system C_PushServer_Heartbeat
```

Pour modifier la valeur (en milli secondes) :

```
tool set system C_PushServer_Heartbeat 1800000
```

Si vous voulez monter la valeur au delà de 30 minutes, il faudra modifier la configuration du serveur pour étendre la temporisation de PHP. Si le serveur web fonctionne en mode ISAPI (par défaut sur Windows), ce n'est pas nécessaire.

Si le mode du serveur Web a été basculé à FastCGI ou si vous fonctionnez sous Linux où ce mode est par défaut, il faut effectuer les modifications suivantes :

© IceWarp France / DARNIS Informatique

Toute reproduction interdite sans accord d'IceWarp France

Dans ...\config\webserver.dat modifier la valeur de la période en milli secondes (1800000 ici) :

Sous Linux :

```
<ITEM>
 <TITLE>[activesync]</TITLE>
 <MODULE>(fastcgi)var/phpsocket;scripts/phpd.sh;1800000</MODULE>
</ITEM>
```

Sous Windows :

```
<ITEM>
 <TITLE>[activesync]</TITLE>
 <MODULE>(fastcgi);php\php.exe;1800000</MODULE>
</ITEM>
```

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Accès mail au GroupWare

L'accès mail au GroupWare permet d'étendre la compatibilité des mobiles ActiveSync aux ressources qui ne sont pas nativement supportées par ActiveSync tels que les fichiers, les notes et les tâches. Ces données sont implicitement converties en messages mails et rendus disponibles sur le client mail du mobile dans le dossier correspondant exactement comme sur le Client Web ou Outlook.

Grâce à l'accès mail au GroupWare, ces éléments sont synchronisés en toute sécurité vers le mobile comme des mails (avec ou sans le Push) avec tous les détails, catégories, participants et fichiers attachés, là ou il aurait fallu installer des logiciels spécialisés sur le mobile pour permettre cette synchronisation (comme WebDav ou SyncML).

Comment ça marche :

- Les dossiers GroupWare sont mappés sur des dossiers IMAP
- Les éléments GroupWare sont convertis en mails
- Ils sont accessibles sur tout client qui supporte les sous dossiers mails (voir la matrice de compatibilité)
- La procédure est complètement transparente pour tous les mobiles qui ne gèrent pas ces types de données.
- **Notes** : elles contiennent toutes les informations d'origine, sont triées par date de modification et comprennent les fichiers attachés
- **Tâches** : ne sont pas synchronisées si le filtre des mails est inférieur à 7 jours
- **Fichiers** : la taille limite est fixée uniquement par les capacités du mobile
- La catégorie est conservée dans le champ émetteur du message
- La synchronisation ne s'effectue que dans le sens serveur vers mobile.

Sur les mobiles Windows et quelques autres, il faut cocher les dossiers qui doivent être synchronisés dans la configuration d'ActiveSync.

L'application mail de l'iPhone liste tous les dossiers et sous-dossiers qui sont directement disponibles pour la synchronisation.

Certains mobiles ne listent que les dossiers de base (Inbox, Brouillons, envoyés, corbeille) et par conséquent, l'accès mail au GroupWare ne peut fonctionner ; il est cependant possible dans certains cas de déplacer les mails en question dans l'Inbox de façon à les rendre accessibles.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Durée de vie de la batterie

Pour préserver la batterie, il est préférable de ne pas valider le Push. Sur certains mobiles, il est possible de n'enlever le Push que pour les mails et le laisser pour la synchronisation des contacts et calendriers. Cela provoque une légère amélioration de la durée de vie de la batterie.

Le push ne génère que peu de trafic tant qu'il n'y a pas de données à synchroniser. C'est le maintien permanent de la connexion qui consomme de la puissance.

Vous pouvez désactiver la connexion WiFi si la connexion 2G/3G fonctionne. Désactivez au minimum la recherche de nouveaux réseaux WiFi si possible.

Configurez votre propre réseau mobile manuellement et supprimez la recherche d'autres réseaux, sauf si vous voyagez.

Désactivez Bluetooth sauf si vous utilisez un casque

Si vous pouvez régler la période de pulsation, allongez-la à une valeur proche de 30 minutes. Si toutefois vous constatez un ralentissement des notifications, conservez les valeurs par défaut ou automatique.

Ne modifiez pas la période de pulsation sur le serveur à moins d'une très bonne raison. La baisser augmente la fréquence d'envoie de Pings vers le serveur ce qui augmente la consommation de la batterie.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Éléments de sécurité

Établissez une politique garantissant des mots de passe forts (cf. chapitre sur la stratégie de sécurité).

Demandez aux utilisateurs de toujours valider le cryptage SSL. Installez un certificat signé (Verisign, DoCoMo,...) sur le serveur (cf. § sur SSL).

Utilisez des applications anti spam et anti virus sur le serveur de façon à filtrer les messages malicieux.

Utilisez des applications de cryptage pour les informations sensibles stockées sur carte mémoire.

Ne mettez jamais les mots de passe, PIN et autres informations sensibles sur votre mobile. Si besoin, utilisez un gestionnaire de mots de passe qui permet de définir des mots de passe forts, de faire des une remise à zéro du mobile sur des erreurs d'entrées du mot de passe et de se synchroniser avec le logiciel d'une machine de bureau pour ne pas perdre les données en cas de mobile perdu, volé, détruit ou effacé.

Désactivez le mode découverte de Bluetooth et ne le valider qu'en cas d'appairage avec un casque ou un autre mobile.

Envisagez d'installer un anti virus sur le mobile, spécialement sur les mobiles Windows.

Utilisez les modalités de diffusion des stratégies de sécurité à travers l'entreprise :

- Réglez une temporisation d'inactivité suffisamment courte avant le blocage du mobile
- Exigez l'entrée du PIN pour le déblocage
- Validez la remise à zéro du mobile en cas de tentatives erronées de déblocage
- Exigez une longueur et une force minimum du PIN et une durée d'expiration.

Demandez aux utilisateurs d'appliquer les mesures de sécurité eux mêmes, même s'ils ne sont pas soumis à la stratégie de sécurité de l'entreprise.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Découverte intelligente

Présentation

Compte tenu du nombre de plus en plus important de services et de protocoles utilisés actuellement, l'utilisateur final a toujours un doute sur la façon de configurer ses applications clientes (emails, mobiles, VoIP...). L'administrateur est donc amené à utiliser différents outils de configuration de masse ou à créer des modes d'emploi très détaillés pour l'utilisateur final.

C'est aussi une grande perte de temps et une solution pour simplifier cette étape était donc nécessaire.

La découverte intelligente est un mécanisme qui permet à toute application cliente, une fois qu'elle a fourni son adresse mail et son mot de passe et qu'elle a été authentifiée par le serveur de recevoir une liste complète des protocoles, ports, URL et adresses serveurs disponibles. Les communications sont cryptées par SSL et le certificat SSL permet de valider le nom du serveur. L'utilisateur peut donc démarrer très rapidement et en fournissant très peu d'informations de configuration.

La découverte intelligente pour ActiveSync est compatible à 100% avec la technologie Microsoft de découverte automatique. Microsoft a implémenté la découverte automatique dans le serveur Exchange uniquement pour les clients Outlook et les mobiles Windows Mobile. IceWarp va plus loin en étendant la découverte automatique à ses clients Web, IM et SIP et à l'agent de notification. Pratiquement tout protocole peut être configuré par la découverte intelligente du moment que le client associé la supporte.

Lien MSDN :

http://msdn.microsoft.com/en-us/library/cc433481.aspx

http://msdn.microsoft.com/en-us/library/cc463896.aspx

Test :

https://www.testexchangeconnectivity.com/

Comment ça marche

Une fois qu'elle connaît l'adresse mail et le mot de passe, l'application cliente va essayer de contacter le serveur par une requête HTTP GET en utilisant le nom de domaine de l'adresse mail comme base de départ. La communication est sécurisée par le certificat SSL (cryptage et validation de l'hôte). Ceci suppose qu'un certificat SSL reconnaissable par le mobile est installé sur le serveur. Si l'URL n'existe pas ou retourne une erreur, le client réessaye l'autre URL selon le même principe jusqu'à ce que le service de découverte intelligente soit reconnu.

Ces URL sont compatibles avec les mobiles ActiveSync (domain.com est le domaine de l'utilisateur contenu dans l'adresse mail) :

https://autodiscover.domain.com/autodiscover/autodiscover.xml

https://domain.com/autodiscover/autodiscover.xml

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Le client va alors s'authentifier par une authentification HTTP en utilisant la même adresse mail et le même mot de passe et, en cas de succès, le serveur renvoie les détails de la configuration sous forme d'un fichier texte XML. Le client lit la partie correspondant aux services qu'il fournit et se configure en conséquence sans l'intervention de l'utilisateur.

Requêtes

1 - Tentative avec un domaine de découverte intelligente

Le client émet une simple requête HTTP GET à :

https://autodiscover.domain.com/autodiscover/autodiscover.xml

Une demande d'authentification est retournée par le serveur. Une fois l'authentification faite, le serveur renvoie une réponse XML.

2 - Tentative sur le domaine

Si l'URL précédente n'existe pas ou retourne une erreur, une deuxième tentative est effectuée sur l'URL :

https://domain.com/autodiscover/autodiscover.xml

3 - Tentative par les enregistrements MX

S'il y a de nouveau échec, le client peut faire une recherche des enregistrements MX du domaine. Il contacte tous les serveurs de la liste dans l'ordre de préférence et essaye de les contacter par une URL de la forme :

https://mxhost1/autodiscover/autodiscover.xml

https://mxhost2/autodiscover/autodiscover.xml

NOTE : cette étape est spécifique des clients développés par IceWarp et ne suit pas la spécification originale de Microsoft.

Réponse

Lorsqu'un HTTP 200 OK est reçu avec un contenu *Content-Type: text/xml* la structure suivante est renvoyée :

...

<Autodiscover>

<Response>

...

<Culture>en:en</Culture>

<User>

<DisplayName>John Doe</DisplayName>

<EMailAddress>john@doe.com</EMailAddress>

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

...

</User>

...

<Account>

...

<Protocol>

<Type>MobileSync</Type>

<Server>http://localhost/Microsoft-Server-ActiveSync</Server>

<Name>http://localhost/Microsoft-Server-ActiveSync</Name>

<LoginName>john@doe.com</LoginName>

</Protocol>

...

<Protocol>

<Type>XMPP</Type>

<Server>localhost</Server>

<Port>5222</Port>

<LoginName>john@doe.com</LoginName>

</Protocol>

...

</Account>

...

</Response>

</Autodiscover>

Chaque type de serveur contient ces attributs. Certains sont optionnels, certains ne s'appliquent qu'à certains types.

<Type> - ID du protocole

<Server> - Adresse serveur ou URL

<Port> - Port pour le nom d'hôte du service

<LoginName> - Nom d'utilisateur pour l'authentification

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Configuration

1 - l'administrateur doit s'assurer de l'existence d'au moins un des enregistrements DNS :

Enregistrement A : autodiscover.domain.com (en général, il n'existe pas)

Enregistrement A : domain.com (le domaine est aussi le nom d'hôte du serveur où tournent tous les services ; généralement, il n'existe pas pour un serveur de base mais peut avoir été créé pour les services Web, XMPP ou SIP.)

Il peut utiliser l'outil dnsquery fourni avec le serveur IceWarp pour vérifier les enregistrements A si la découverte intelligente ne fonctionne pas.

Note : pour l'agent de notification et autres clients natifs d'IceWarp, l'enregistrement n'a pas besoin d'être dans l'enregistrement A. Ces clients vont aussi tester les serveurs contenus dans les enregistrements MX. Donc, si les mails fonctionnent, l'agent de notification réussira forcément à se configurer. Par contre, pour ActiveSync, un des enregistrements A ci-dessus doit exister.

2 - un certificat valide issu d'une autorité de certification doit avoir été installé sur le serveur pour que la découverte intelligente fonctionne avec l'iPhone. Les mobiles Windows ont besoin d'un certificat local auto signé ou issu d'une autorité de certification en correspondance avec le certificat installé sur le serveur. Dans le cas contraire, la découverte intelligente va échouer à cause d'une connexion non sécurisée et non authentifiée avec le serveur

3 - Dans la console d'administration Système -> Services -> Contrôle -> propriétés, le port SSL doit être à 443. La découverte automatique ne fonctionnera pas sinon dans la plupart des cas.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

Liste d'adresse globale (GAL)

La liste d'adresse globale (Global Address List (GAL) ou Global Address Book) est un service d'annuaire inclus dans le système de messagerie Microsoft Exchange. Le GAL contient les informations sur les utilisateurs de la messagerie, les groupes partagés et autres ressources Exchange.

Qu'est-ce le GAL sur le serveur IceWarp

- Tout dossier partagé de contacts ayant l'indicateur GAL
- Un compte utilisateur qui contient un dossier de contacts partagé marqué GAL
- Un dossier public qui contient un dossier public de contacts marqué GAL
- Le GAL peut être alimenté automatiquement à partir des membres d'un groupe
- Il peut y a voir plusieurs dossiers GAL (un pour chaque dossier public) et l'utilisateur peut les consulter sur les mobiles Windows, iPhones ou Blackberry comme s'ils ne formaient qu'un seul dossier.
- Avoir plusieurs GAL est intéressant pour les utilisateurs qui font partie de plusieurs groupes.
- Le GAL peut contenir des photos, des certificats et d'autres ressources associées avec les contacts.

Comment créer un GAL

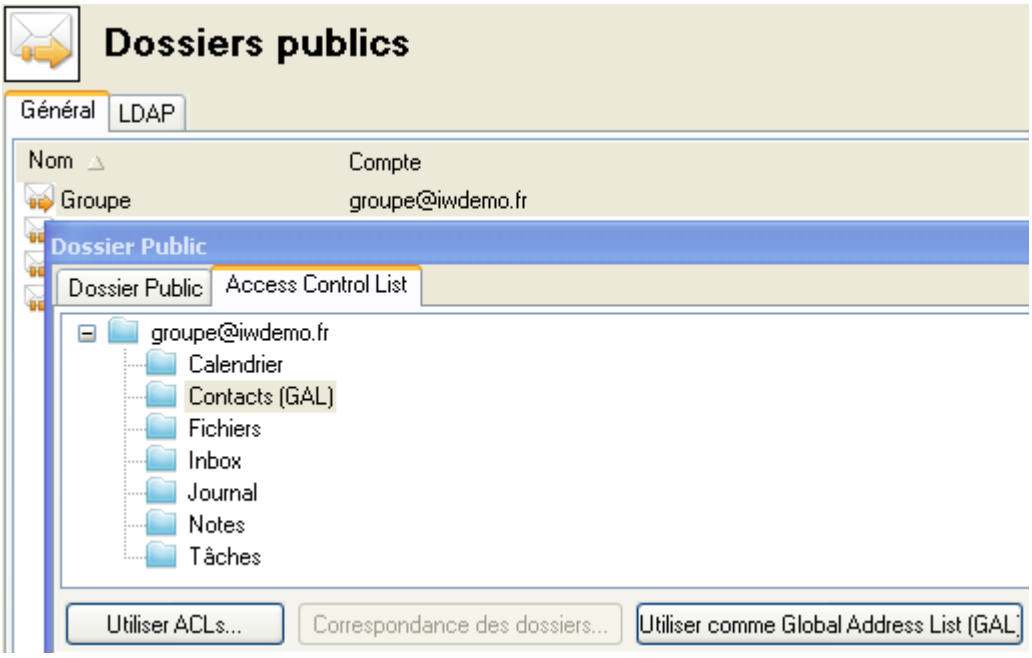
Automatiquement

Créer un nouveau compte de type groupe sur la console d'administration, cocher l'option "Créer un dossier public", donner un nom au dossier et cocher l'option "Mettre tous les membres dans la Global Address liste (GAL)". Allez sur l'onglet Membres, cliquez sur Ajouter... puis ajoutez tout compte du serveur que vous désirez et confirmer en cliquant sur "Sélectionner compte". Répétez l'opération jusqu'à ce que le groupe soit complet. Un accès en mode lecture est suffisant pour les utilisateurs du GAL.

Manuellement

On suppose que vous avez un compte utilisateur, un compte groupe ou un compte public contenant un dossier contacts partagé que vous voulez modifier en GAL. Allez dans la console d'administration dans **GroupWare -> Dossiers publics**, sélectionnez le compte en question puis le bouton Modifier... et l'onglet Access Control List. Sélectionnez le dossier contacts puis le bouton "Utiliser comme Global Address List (GAL)". L'indicateur GAL apparaît alors à côté du dossier.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France



SmartSync

SmartSync est une extension du protocole Exchange ActiveSync complètement transparente pour les clients. Elle est similaire à la fonction "suspend and resume" de SyncML et est capable de gérer les situations où une erreur réseau apparaît au moment où le serveur répond à une requête du client. Le client ne peut pas s'apercevoir d'une erreur tant que la liaison n'est pas tombée au niveau TCP/IP comme lorsque la temporisation de la session déclenche ou que l'instance PHP se termine.

SmartSync est lancé dès que le client envoie une requête avec une clé de synchronisation égale à la précédente requête. Ceci indique que la réponse du serveur n'est pas parvenue au client et que celui-ci n'a donc pas incrémenté la clé de synchronisation. Le serveur Exchange initie alors une synchronisation complète à partir de ce point afin d'éviter une perte de donnée ou une incohérence due à une évolution simultanée d'un élément côté serveur ou côté client.

En mode SmartSync, le serveur IceWarp ActiveSync renvoie une réponse d'état à toute les requêtes incomplètes précédentes de type ajout/modification/suppression ou une réponse de modification si les informations ont changées sur le serveur pendant l'intervalle ; les conflits sont traités en accord avec la configuration utilisateur ou la politique par défaut. S'il y a eu des changements côté client pendant ce temps, le serveur confirme le processus de synchronisation et les changements apparaitront après la reprise normale.

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France

La synchronisation reprend alors normalement. SmartSync peut être activé aussi souvent que de besoin et est capable de reprendre la synchronisation même si toutes les synchronisations sont incomplètes.

Le log commenté ci-dessous illustre une synchronisation interrompue suivie du changement d'un élément sur le serveur (le mobile client est un iPhone) :

```
a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:01 <<< Sync
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>31</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <DeletesAsMoves/>
      <GetChanges/>
      <WindowSize>50</WindowSize>
      <Commands>
        <Add>
          <ClientId>26477</ClientId>
          <ApplicationData>
            <FileAs xmlns="Contacts:">Alex</FileAs>
            <LastName xmlns="Contacts:">Alex</LastName>
            <Picture xmlns="Contacts:"/>
          </ApplicationData>
        </Add>
      </Commands>
    </Collection>
  </Collections>
</Sync>

<!-- Le client a bien ajouté un élément mais le serveur n'a pas répondu à cause d'une erreur -->

a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:43 <<< Sync
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>31</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <DeletesAsMoves/>
      <GetChanges/>
      <WindowSize>50</WindowSize>
    </Collection>
  </Collections>
</Sync>

<!-- Le client continue mais avec la même clé de synchronisation (Synckey), SmartSync est lancé, il y a eu un changement sur le serveur -->

a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:43 >>> 200 OK
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>32</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <Status>1</Status>
      <Responses>
        <Add>
          <ClientId>26477</ClientId>
          <ServerId>3b137c61c028</ServerId>
          <Status>1</Status>
        </Add>
      </Responses>
```

© IceWarp France / DARNIS Informatique

Toute reproduction interdite sans accord d'IceWarp France

```
   </Collection>
  </Collections>
</Sync>
```

<!-- Le serveur envoie OK pour reprendre la synchronisation de l'élément précédent avec une nouvelle clé SyncKey -->

```
a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:36:12 <<< Sync
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>32</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <DeletesAsMoves/>
      <GetChanges/>
      <WindowSize>50</WindowSize>
    </Collection>
  </Collections>
</Sync>
```

<!-- Le client demande une synchronisation incrémentale standard -->

```
a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:36:34 >>> 200 OK
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>33</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <Status>1</Status>
      <Commands>
        <Change>
          <ServerId>3b137c61c028</ServerId>
          <ApplicationData>
            <LastName xmlns="Contacts:">Alex E</LastName>
            <FileAs xmlns="Contacts:">Alex</FileAs>
          </ApplicationData>
        </Change>
      </Commands>
    </Collection>
  </Collections>
</Sync>
```

<!-- Le serveur envoie l'élément modifié au client -->

© IceWarp France / DARNIS Informatique
Toute reproduction interdite sans accord d'IceWarp France