
Le serveur de communication IceWarp

Guide Exchange ActiveSync

Version 12



15 février 2021

Sommaire

Guide Exchange ActiveSync 2

Introduction	2
Présentation de Exchange ActiveSync	2
Configuration du serveur	5
Gestion ABQ.....	7
Menu GroupWare -> ActiveSync	9
Stratégie de sécurité.....	14
Effacement local ou distant de l'appareil	14
Définition de la stratégie.....	15
Héritage des stratégies.....	16
Acceptation des stratégies	17
Exclusion de la politique de sécurité	17
Suppression de la stratégie de sécurité.....	17
Références de la configuration.....	18
Gestion des appareils	24
Configuration des appareils.....	27
Configuration	27
Problèmes de fonctionnement	29
En cas de problème de fonctionnement.....	29
Réinitialiser la base de données ActiveSync.....	32
Changer la période de pulsation.....	33
Accès mail au GroupWare	34
Durée de vie de la batterie.....	35
Éléments de sécurité.....	36
Découverte intelligente.....	37
Présentation.....	37
Comment ça marche	37
Configuration	39
Liste d'adresse globale (GAL)	41
Comment créer une GAL.....	41
SmartSync.....	42

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 appareil utilisant ActiveSync et qui souhaitent le configurer, peuvent aller directement au chapitre [Configuration de l'appareil](#). 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 appareils implémentant ce protocole.

Microsoft 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 appareils d'avoir un accès centralisé via le Serveur IceWarp aux informations les plus importantes de l'organisation. IceWarp et ActiveSync permettent aux utilisateurs d'appareils d'avoir accès à leur courrier électronique, calendrier, contacts et tâches quand ils sont connectés par le réseau mobile 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) 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.

Marques et recours

Windows, Exchange, SQL Server, ActiveSync, AutoDiscover, DirectPush, RemoteWipe sont des marques déposées de Microsoft Corporation. iPhone, iSync, Mac, OS X sont des marques déposées d'Apple Inc. Android est une marque déposée de Google Inc.

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 tous les appareils dont l'OS est OS X ou Android de version récente.

Si ActiveSync n'est pas directement supporté, un logiciel tiers doit être installé sur l'appareil pour permettre la synchronisation avec ActiveSync.

Caractéristiques

ActiveSync permet les synchronisations suivantes (ces informations ne sont pas forcément supportées par l'appareil lui-même) :

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

Caractéristiques avancées et gestion de l'appareil :

- 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 l'appareil le permet
 - Dossiers sélectionnés pour la synchronisation avec des applications internes
- Gestion des dossiers
 - Ajout, suppression, renommage, déplacement dans l'arbre des dossiers
- Manipulation complète des emails (envoi, réponse, transfert, marquage...)
- Synchronisation des indicateurs (marques, répondu, transféré)
- 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 de l'appareil
 - Liste de tous les appareils connectés par domaine/utilisateur avec le nom du modèle
 - Effacement distant de l'appareil pour supprimer toutes les données d'un appareil volé
- Consultation à distance d'un annuaire d'entreprise (GAL)
 - Auto complétion des adresses mail
 - Consultation des adresses des contacts
- L'utilisateur a accès à sa liste d'appareils, certains éléments de stratégies et la commande d'effacement distante.
- 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 de l'appareil, le nombre maximum de tentatives mauvaises, l'effacement local de l'appareil en cas de compromission.
 - Tous les paramètres de sécurité sont implémentés du côté serveur mais leur fonctionnalité réelle dépend du côté appareil.

Limitations

Les invitations au format TNEF (envoyées par Outlook) ne sont pas supportées (il n'est pas possible d'y répondre ni par le serveur ni par le Client Web).

Avantages du push direct

- Notification immédiate des messages
- Adapté aux connexions lentes
- 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 l'appareil
- Indépendant de la taille limite des mails
- Pas d'applications nécessaires, fonctionne dès la mise en route
- Configuration simple
- Accès sécurisé par SSL (HTTPS)

Explication sur la **synchronisation des dossiers** : le document suivant donne des détails très précis sur la façon dont les dossiers sont synchronisés (§ Folder Synchronization explanation) :

<http://www.icewarp.com/download/documentation/server/mobility/V%2012%20ActiveSync%20Guide.pdf>

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 encore au moins un compte. 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](#).
Un utilisateur avec un seul compte peut connecter autant d'appareils qu'il le désire avec une seule licence.
Cliquer sur la ligne Licence du menu Aide de la console pour avoir les licences disponibles. En cliquant sur ActiveSync, on obtient la liste des utilisateurs de licences.

2. Dans Système -> Services, démarrer **Notification GroupWare**. Dans la fenêtre des propriétés de ce service, vérifier que le port par défaut (32002) n'est pas bloqué par un autre service local. Vous pouvez changer ce port. Il n'y a pas besoin d'ouvrir les pare-feux car ce port est uniquement interne. Ce service collecte toutes les modifications à partir de IMAP/GroupWare dans un flux UDP et est utilisé par ActiveSync et Outlook Sync pour activer la synchronisation. N'activer le journal de ce service que de façon temporaire car il est très prolix.

Il est possible de ne pas valider ce service pour économiser de la ressource sur le serveur et sur les appareils. Dans ce cas, il n'y a pas de push direct.

Si vous utilisez le partage de charge, la notification GroupWare doit être désactivée sur les serveurs secondaires. De ce fait, toutes les notifications sont prises en charge par le serveur principal et il n'y a pas de partage de charge pour ce service. Si ActiveSync est activé sur le serveur secondaire, il n'y aura pas de push direct.

3. 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 peut fonctionner avec un service Contrôle sur d'autres ports (par exemple 32000 et 32001) il faut alors les indiquer explicitement dans la configuration du poste.

4. Pour l'accès à la **liste d'adresse globale** (GAL), vous devez avoir un dossier public marqué GAL. Pour avoir accès à la GAL, la case "Dossiers publics" de l'appareil doit être cochée. [Voir le paragraphe sur les dossiers publics GAL pour plus de détails.](#)
5. Dans le menu **Système -> Services -> IMAP**, vérifiez que le service tourne et que les ports spécifiés sont les ports 143 et 993 (SSL).
Note : si SSL n'est pas utilisé, toutes les données y compris les mots de passe sont transmis en clair.
6. 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](#).
7. 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>:<port>/Microsoft-Server-ActiveSync>". Le port n'est pas utile si les ports par défaut sont utilisés (80 et 443).
8. Dans l'**onglet Stratégies du compte** utilisateur, vérifier que la case ActiveSync est bien cochée.
9. 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](#).
10. 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 Let's Encrypt par exemple.

Gestion ABQ

Termes

- ABQ = Autoriser, Bloquer, mettre en Quarantaine
- La gestion des ABQ comprend :
 - Les règles d'accès aux appareils (**règles ABQ**)
 - Les informations (**paramètres**) envoyées à un appareil par des commandes de configuration.
- Une règle ABQ standard consiste en un triplet comprenant un **paramètre**, sa **valeur** et **l'ABQ**.
- Les paramètres sont : **Type** d'appareil, **Modèle** d'appareil, Système d'opération (**OS**)
- La valeur est une chaîne sensible à la casse
- L'ABQ est une de ces valeurs : **Autoriser, Bloquer, Quarantaine**
- Une règle ABQ peut avoir une **description** et peut être **désactivée**.

Types de règles ABQ

- Une règle ABQ simple et obligatoire sans paramètre (Règle globale)
- Les règles ABQ standards optionnelles qui ne sont actives que côté serveur (Règle serveur)
- Une règle ABQ optionnelle simple sans paramètre pour tous les domaines et tous les utilisateurs (Règle domaine et règle utilisateur).

ABQ des nouveaux appareils

- Exigences
 - L'appareil est authentifié
 - ActiveSync est valide pour cet utilisateur
 - L'appareil répond aux exigences de sécurité
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau utilisateur (règle utilisateur) alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.

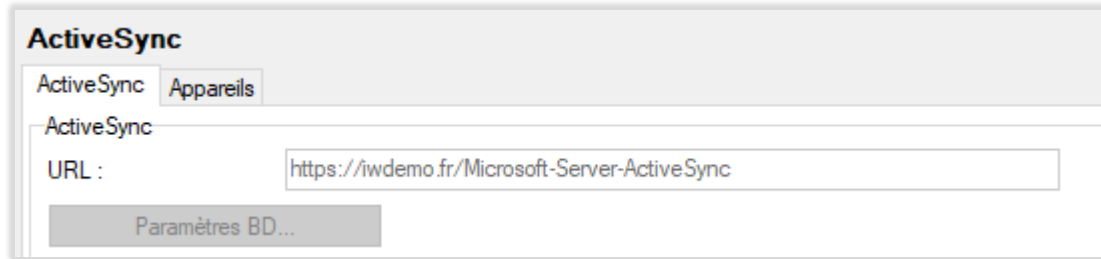
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau domaine (**règle domaine**) alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau serveur (**règle serveur**) par un paramètre OS alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau serveur (**règle serveur**) par un paramètre Modèle alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau serveur (**règle serveur**) par un paramètre Type alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.
- S'il y a une règle qui autorise, bloque ou quarantaine l'appareil au niveau global (**règle globale**) alors, donner l'accès, bloquer ou mettre en quarantaine l'appareil. Passer ensuite à l'étape suivante.
- Comment sont comparés les paramètres envoyés par l'appareil avec les règles serveur :
 - La comparaison est sensible à la casse
 - Si la valeur du paramètre est par exemple "Android" alors la valeur envoyée par l'appareil est comparée pas à pas avec les suivants : "android", "andro", "andr", "and", "an", "a".

Les états ABQ

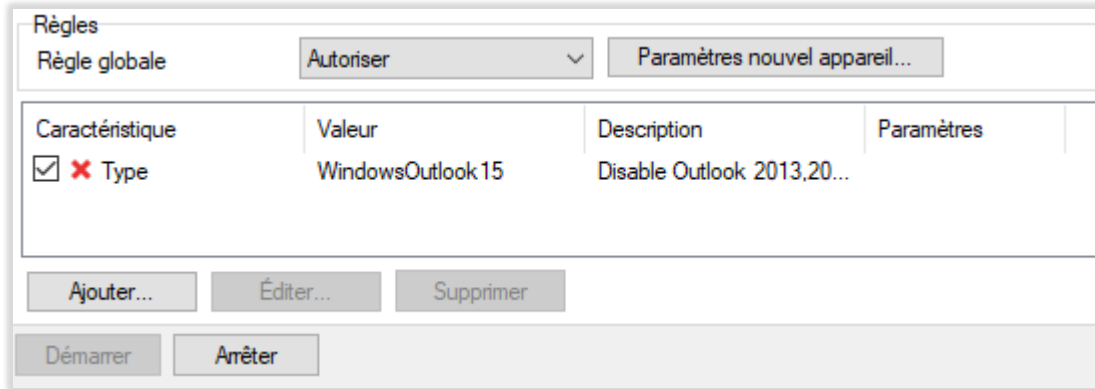
- Autoriser
 - Toutes les fonctions EAS sont autorisées
 - Ces appareils peuvent être bloqués par l'administrateur
- Bloquer
 - Renvoie une erreur "accès interdit" à l'appareil
 - Les appareils bloqués ne sont pas listés dans le Client Web
 - Les appareils bloqués peuvent être autorisés par l'administrateur
 - Ne pas confondre ce blocage avec celui généré par un Hard Wipe ou un Soft Wipe
- Mettre en quarantaine
 - Seuls les dossiers par défaut sont synchronisés
 - Un seul sens de synchronisation est autorisé (client vers serveur)
 - L'utilisateur reçoit un message d'information sur cette situation.




- Les appareils en quarantaine ne sont pas listés dans le Client Web
- Les appareils en quarantaine peuvent être autorisés ou bloqués par l'administrateur

Menu GroupWare -> ActiveSync



Champ	Description
URL	<p>L'URL est constituée :</p> <ul style="list-style-type: none"> • De l'adresse du serveur ou son alias : iwdemo.fr dans l'exemple ci-dessus <p>Ce nom doit être configuré dans le client avec le même nom sinon, la synchronisation ne fonctionnera pas.</p> <p>Si le port utilisé n'est pas un port par défaut (80 pour HTTP, 443 pour HTTPS) il faut l'indiquer après le nom du serveur.</p> <ul style="list-style-type: none"> • Du chemin spécifié par Microsoft : Microsoft-Server-ActiveSync <p>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 l'appareil.</p>
Paramètres BD...	<p>Ce bouton donne accès aux propriétés de la base de données du cache d'ActiveSync. Cet accès n'est possible que si le service est arrêté.</p> <p>Note : cette base et la base GroupWare ne peuvent pas être communes à cause d'une table ayant le même nom.</p>

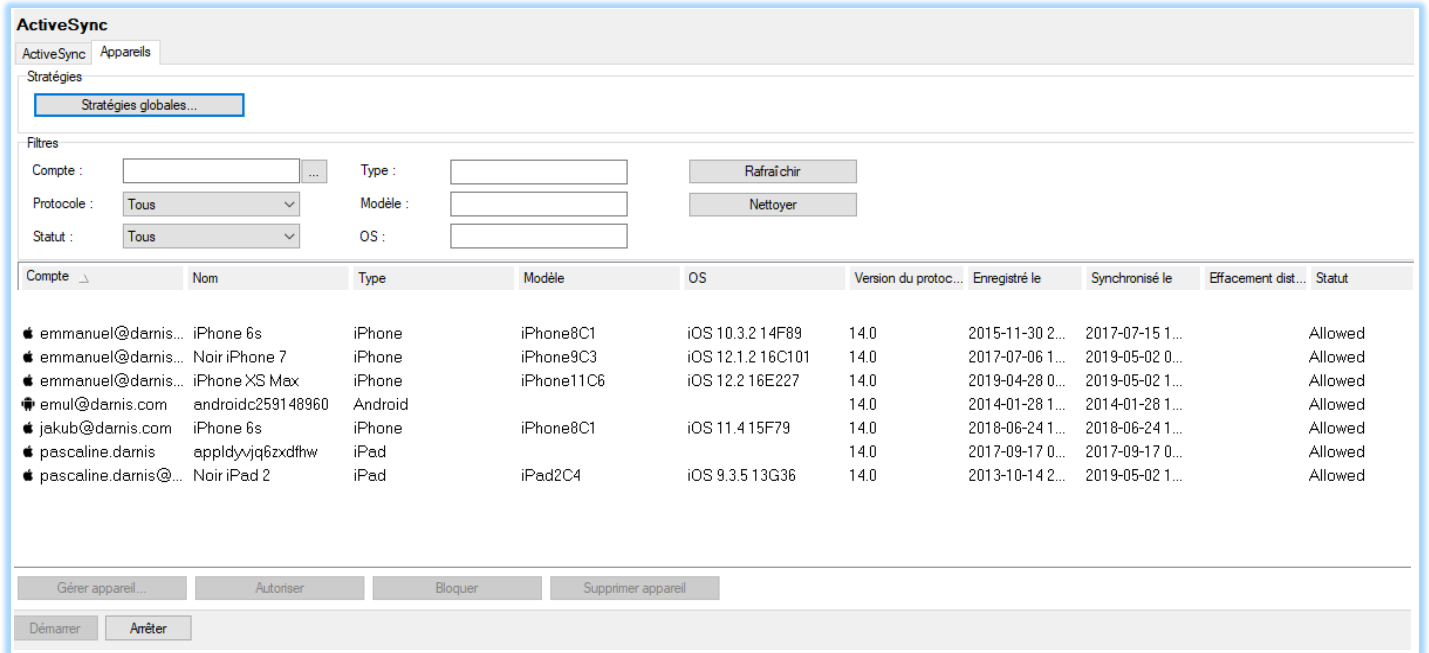


Champ	Description
Règle globale	Sélectionner la règle ABQ par défaut pour les appareils qui n'obéissent pas aux règles données en dessous
Paramètres nouvel appareil...	Ce bouton ouvre la fenêtre de paramétrage des nouveaux appareils. Voir le paragraphe sur la gestion des appareils.
Icones de la liste	 Appareil autorisé  Appareil bloqué  Appareil mis en quarantaine
Ajouter	Pour ajouter une nouvelle règle
Editer	Pour modifier une règle
Supprimer	Pour supprimer une règle Pour désactiver une règle sans la supprimer, il suffit de décocher la case à gauche de la ligne

Fenêtre des règles

Champ	Description
Actif	Pour activer la règle
Description	Courte description
Caractéristiques	Sélectionner le critère de la règle. Les critères sont, dans l'ordre d'affichage : OS, Modèle, Type
Valeur	Entrer la valeur appropriée.
Action	Action à exécuter.
Paramètres nouvel appareil	Ouvre la fenêtre de paramétrage de l'appareil. Pour plus de détails, voir le paragraphe sur la configuration des appareils.

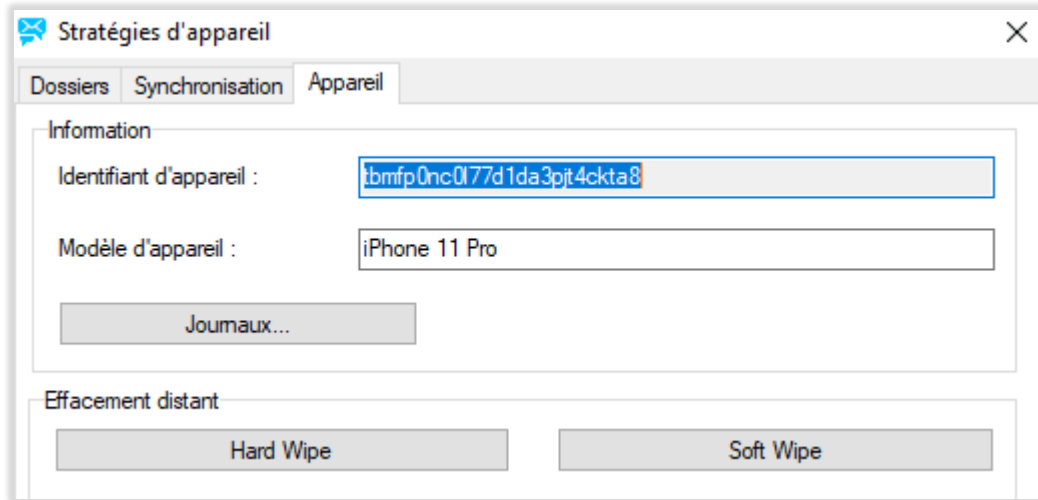
Onglet Appareils



Bouton	Description
Stratégies globales	Permet de configurer la stratégie de sécurité pour tous les appareils au niveau du serveur. Pour plus de détails, voir le paragraphe sur les stratégies de sécurité .
Filtres	Utiliser ce filtre pour lister un sous ensemble des appareils. Rafraîchir permet d'activer le filtre et Nettoyer supprime le filtre.
Gérer appareils	Permet de configurer la stratégie de sécurité pour l'appareil sélectionné. Pour plus de détails, voir le paragraphe sur les stratégies de sécurité .
Autoriser	Autoriser la synchronisation de l'appareil
Bloquer	Bloquer la synchronisation d'un appareil
Supprimer appareil	Cette action enlève l'appareil 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 appareils. Note : cette action n'arrête pas la synchronisation de l'appareil mais la réinitialise.

Règle pour les appareils similaires	Crée une règle pour les appareils similaires.
--------------------------------------------	-----------------------------------------------

Dans les propriétés de l'appareil, on trouve :



Journaux	Ce bouton ouvre la fenêtre des journaux (Etat -> Journaux -> ActiveSync en introduisant le filtre de l'appareil sélectionné.
Hard Wipe	<p>Permet de lancer l'effacement de l'appareil de type Hard Wipe L'appareil est dans ce cas réinitialisé à sa configuration usine par défaut lors de la prochaine connexion de l'appareil au serveur.</p> <p>En cliquant sur ce bouton, un message va vous demander de confirmer que vous souhaitez effacer le contenu de l'appareil. Lorsque l'effacement est initié, son statut apparaît dans la colonne "Effacement distant".</p> <p>Non supporté signifie que l'appareil n'accepte pas l'effacement distant.</p> <p>Attente signifie que la commande sera envoyée à la prochaine synchronisation. Si l'appareil ne traite pas le push ou n'est pas connecté, le serveur doit attendre.</p> <p>Après que l'effacement distant ait été exécuté, l'appareil est supprimé de la liste et le système envoie un message d'acquittement au propriétaire du compte et à l'administrateur. L'appareil réapparaîtra de nouveau dans la liste après la première synchronisation réussie.</p> <p>Note : l'effacement distant est spécifique d'un appareil et non d'un compte. Si un compte a deux appareils, un effacement distant sur un de ses appareils n'effacera pas les données sur l'autre.</p>
Soft Wipe	Permet de lancer l'effacement de l'appareil de type Soft Wipe

Toutes les données relatives à ce compte seront effacées lors de la prochaine connexion de l'appareil au serveur.

Stratégie de sécurité

La stratégie de sécurité permet aux appareils 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 l'appareil. 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 appareils de cette stratégie, à éviter les appareils non compatibles et à mettre à jour les firmware et OS.

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 de l'appareil 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.

Effacement local ou distant de l'appareil

Lorsqu'un appareil 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.

L'effacement d'un appareil localement ou à distance a les mêmes conséquences qu'un reset matériel. L'effacement peut être effectué de deux façon : en écrasant toutes les données, les configurations et les clés privées de l'appareil en inscrivant dans la mémoire une séquence de bits qui rend la relecture des données très difficile ou par un simple effacement logiciel qui est beaucoup moins efficace mais plus rapide.

Notes : Le temps de nettoyage complet d'un iPhone peut atteindre une heure à cause de l'écriture d'une séquence binaire sur toute la mémoire.

Nettoyage local

Le nettoyage local est provoqué sur un appareil 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, l'appareil 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, l'appareil 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 l'appareil la recevra à sa prochaine synchronisation. L'utilisateur de l'appareil ne devrait pas pouvoir empêcher le nettoyage distant (cette possibilité dépend des appareils).

Deux modes sont définis :

Hard Wipe : L'appareil est dans ce cas réinitialisé à sa configuration usine par défaut lors de la prochaine connexion de l'appareil au serveur.

Soft Wipe : Toutes les données relatives à ce compte seront effacées lors de la prochaine connexion de l'appareil au serveur.

Confirmation par mail

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

Restrictions

Les appareils 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 appareils 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 appareil 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 appareils 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 appareil. Les paramètres sont ceux indiqués sur l'écran ci-dessus.

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 l'appareil 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 l'appareil 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.

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

Si la stratégie change, un message avertissant l'utilisateur est envoyé sur l'appareil 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 l'appareil 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 l'appareil 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 appareils de la stratégie de sécurité.

Elle permet de spécifier qu'un appareil d'ancienne génération peut quand même se connecter au serveur alors que les appareils 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 appareil particulier, il suffit de sélectionner cet appareil et de décocher l'option "imposer mot de passe sur appareil". Une commande de suppression de la stratégie de sécurité est alors envoyée à l'appareil et les paramètres par défaut de l'appareil 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.

Stratégies

Les stratégies courantes sont celles du niveau : défaut.

Sécurité Synchronisation Appareils Applications sur mobile

Exiger un mot de passe sur l'appareil

Longueur minimum du mot de passe (caractères) : 4

Refuser les mots de passe simples

Imposer lettres et chiffres

Nombre minimum de caractères de chaque type : 1

Activer la récupération du mot de passe

Mot de passe expire dans (jours) : 1

Appliquer l'historique des mots de passe (nombre) : 1

Délai d'inactivité (minutes) : 5

Effacer les données de l'appareil après échecs (nombre de tentat) : 8

Exiger cryptage sur l'appareil

Exiger cryptage sur la carte de stockage

Rafraîchir paramètres sur appareil (heures) : 24

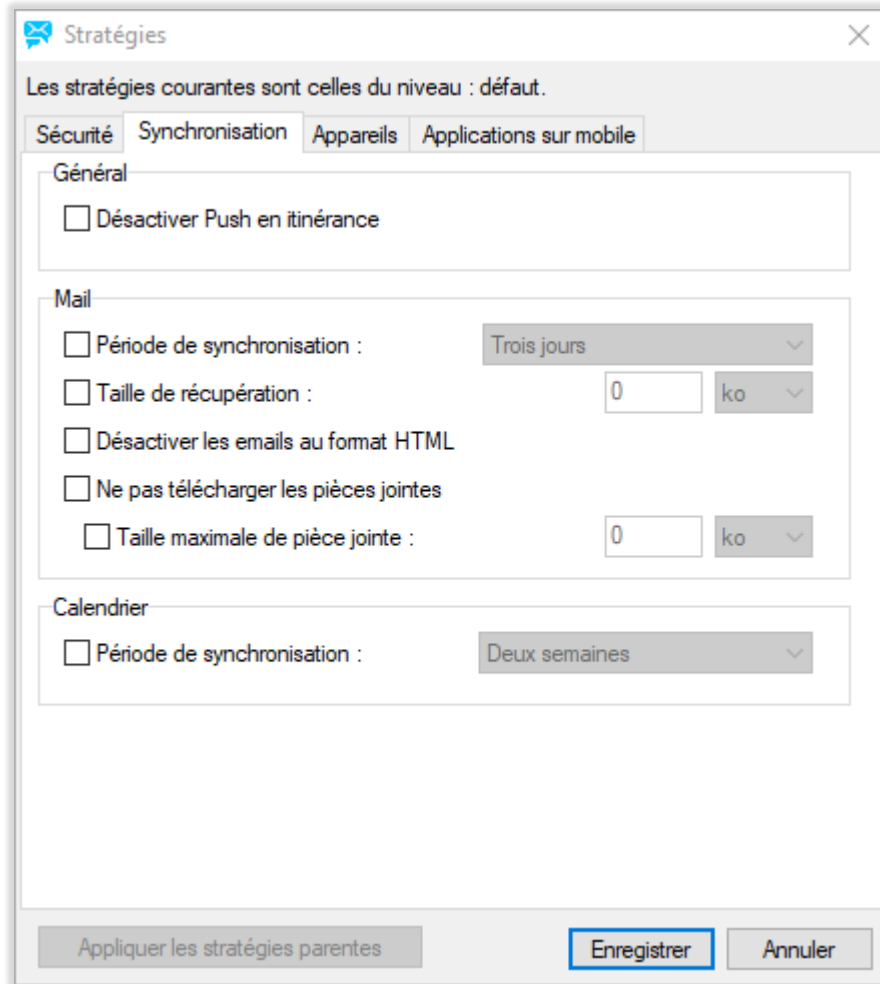
Permettre l'accès aux appareils ne supportant pas les contraintes de sécurité

Appliquer les stratégies parentes Enregistrer Annuler

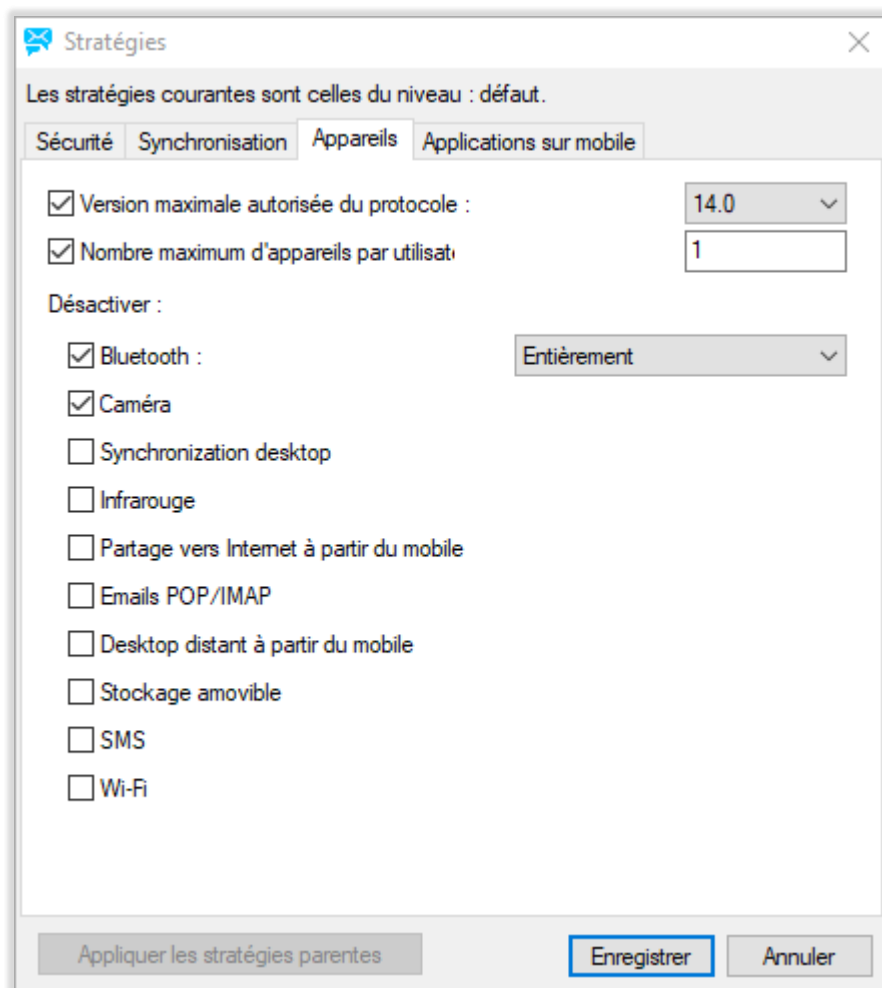
Champ	Description
Libellé en haut de la fenêtre	<p>"Les stratégies sont héritées du niveau défaut/serveur/domaine/utilisateur"</p> <p>Ce libellé indique que la stratégie n'a pas été personnalisée à ce niveau et indique de quel niveau elle hérite (niveau le plus haut).</p> <p>"Pour hériter des stratégies d'un niveau supérieur, cliquez sur le bouton "Hériter" ci-dessous"</p> <p>Ce libellé indique que le niveau a été personnalisé</p> <p>Note : si le bouton "Hériter" est utilisé à un niveau, les paramètres du niveau juste supérieur sont utilisés.</p>

	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	<p>Si cette option est cochée, un mot de passe sera demandé à la mise sous tension et après un certain délai d'inactivité ; les options suivantes deviennent actives et permettent de préciser les conditions d'utilisation du mot de passe. Les paramètres définis ci-dessous prennent le pas sur ceux définis dans l'appareil.</p> <p>Si les options ci-dessous ne sont pas définies, les options par défaut de l'appareil sont prises en compte.</p> <p>Si cette option n'est pas cochée, l'utilisateur de l'appareil peut choisir les options de sécurité qu'il désire.</p>
Longueur min mot de passe (caractères)	Si une valeur est indiquée, le mot de passe choisi par l'utilisateur pour son appareil devra s'y conformer sous peine de rejet par le serveur.
Refuser les mots de passe simples	Permet de refuser de simples mots de passe comme 1234 ou abcd
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 l'appareil.
Nombre minimum de types de caractères	<p>Permet de définir la complexité du mot de passe.</p> <p>Les valeurs autorisées sont de 1 à 4.</p> <p>Les 4 types possibles sont : caractères alphabétiques minuscules, caractères alphabétiques majuscules, chiffres et caractères spéciaux.</p> <p>Par exemple si la valeur vaut 2, un mot de passe avec des minuscules et des chiffres sera accepté.</p>
Activer la récupération du mot de passe	Un mot de passe de récupération est un mot de passe qui est créé par l'appareil et qui permet à l'utilisateur de se connecter une fois sur l'appareil. La fois suivante, l'utilisateur doit créer un nouveau mot de passe et l'appareil crée un nouveau mot de passe de récupération.
Mot de passe expire dans (jours)	<p>Durée de validité d'un mot de passe.</p> <p>0 : pas de limite.</p>
Appliquer l'historique des mots de passe	<p>Cette option mémorise les différents mots de passe utilisés pour éviter leur réutilisation.</p> <p>0 : pas de mémorisation</p> <p>> 0 : Nombre de mots de passe mémorisés</p>
Délai d'inactivité (minutes)	<p>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.</p> <p>Ce délai n'est pas lié au temps d'allumage de l'écran qui est limité pour diminuer la consommation.</p> <p>Le délai peut être positionné de 0 à 9999 minutes</p> <p>0 signifie que le mot de passe sera demandé dès que l'appareil est éteint. S'il l'appareil n'a pas de temporisation d'extinction, le mot de passe ne sera demandé qu'à la mise en route de l'appareil.</p>
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 de l'appareil sera effacée.

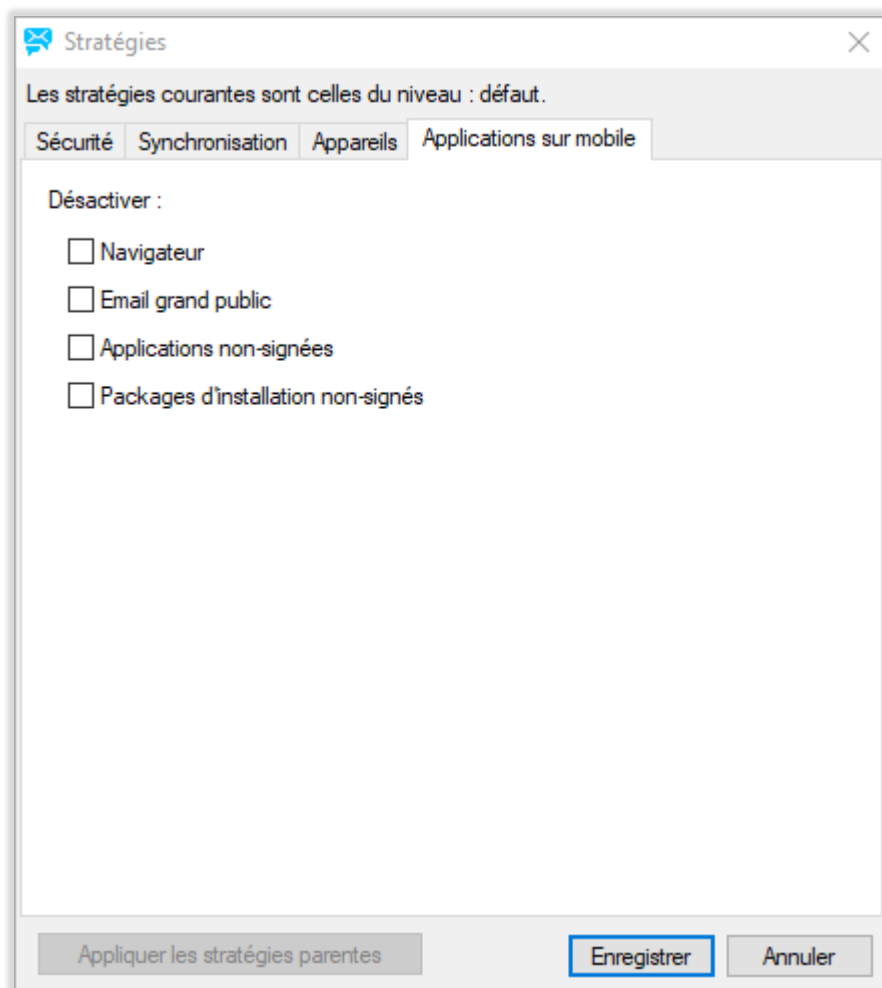
	<p>0 signifie que l'effacement automatique est désactivé et que l'utilisateur ne peut pas l'activer.</p> <p>Si l'option n'est pas cochée, l'option est laissée au libre choix de l'utilisateur de l'appareil.</p>
Exiger cryptage sur l'appareil	Si cochée, l'appareil doit utiliser le cryptage
Exiger cryptage sur la carte de stockage	Si cochée, l'appareil doit utiliser le cryptage y compris sur la carte de stockage.
Rafraîchir paramètres sur appareil (heures)	<p>Spécifie à quel intervalle la stratégie de sécurité sera synchronisée vers l'appareil. 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 à l'appareil.</p> <p>Si l'option n'est pas cochée, la stratégie sera appliquée une seule fois. A la première synchronisation après création du compte sur l'appareil ou à la prochaine synchronisation si le compte existe déjà.</p>
Permettre l'accès à un appareil ne supportant pas les contraintes de sécurité	<p>Si la case est cochée, cela signifie que tous les appareils peuvent se synchroniser avec le serveur. Aussi bien les appareils qui ne supportent pas les stratégies de sécurité que ceux dont l'utilisateur l'a refusée. C'est l'option par défaut.</p> <p>Si la case n'est pas cochée, les appareils 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.</p>
Appliquer les stratégies parentes	Cliquer pour hériter du niveau supérieur.
Enregistrer	Après avoir cliqué sur Enregistrer, la configuration est sauvegardée.
Annuler	Pour quitter la fenêtre sans appliquer les modifications.



Champ	Description
Désactiver Push en itinérance	Si cochée, la synchronisation doit être manuelle en itinérance
Période de synchronisation	Spécifie l'âge maximum des emails à synchroniser
Taille de récupération	Si -1, les emails ne sont pas tronqués Si 0, seule l'entête est envoyé Une autre valeur spécifie la taille à laquelle les messages sont tronqués
Désactiver les emails au format HTML	Si cochée, seuls la partie texte des emails est synchronisée
Ne pas télécharger les pièces jointes	Si cochée, les pièces jointes ne sont pas téléchargées
Taille maximale des pièces jointes	Si cochée, les pièces jointes de taille supérieure à la limite ne sont pas téléchargées.
Période de synchronisation	Permet de spécifier le nombre maximum de jours du calendrier qui seront téléchargés.



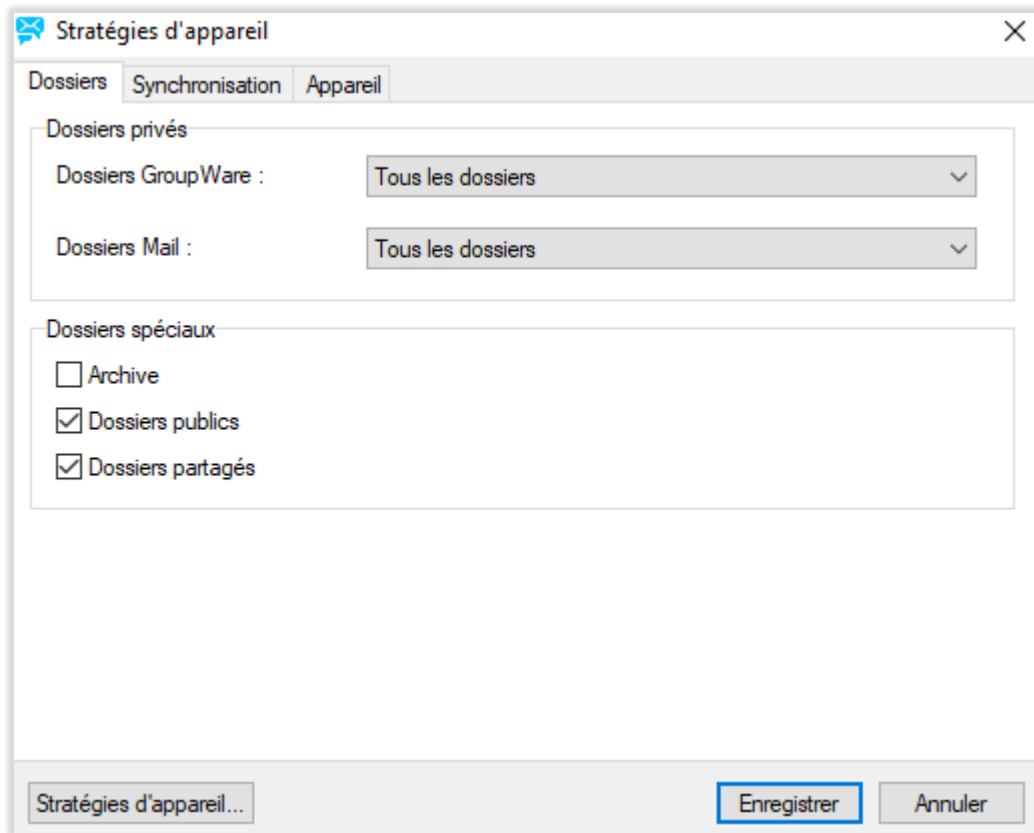
Champ	Description
Version du protocole la plus élevée	Abaisser la version du protocole peut permettre de résoudre certains problèmes de synchronisation
Nombre maximum d'appareil par utilisateur	Limite le nombre d'appareils pour un utilisateur
Désactiver	Permet de désactiver certaines fonctions de l'appareil Pour bluetooth, il faut préciser le niveau



Champ	Description
Désactiver	Permet de désactiver certaines applications.

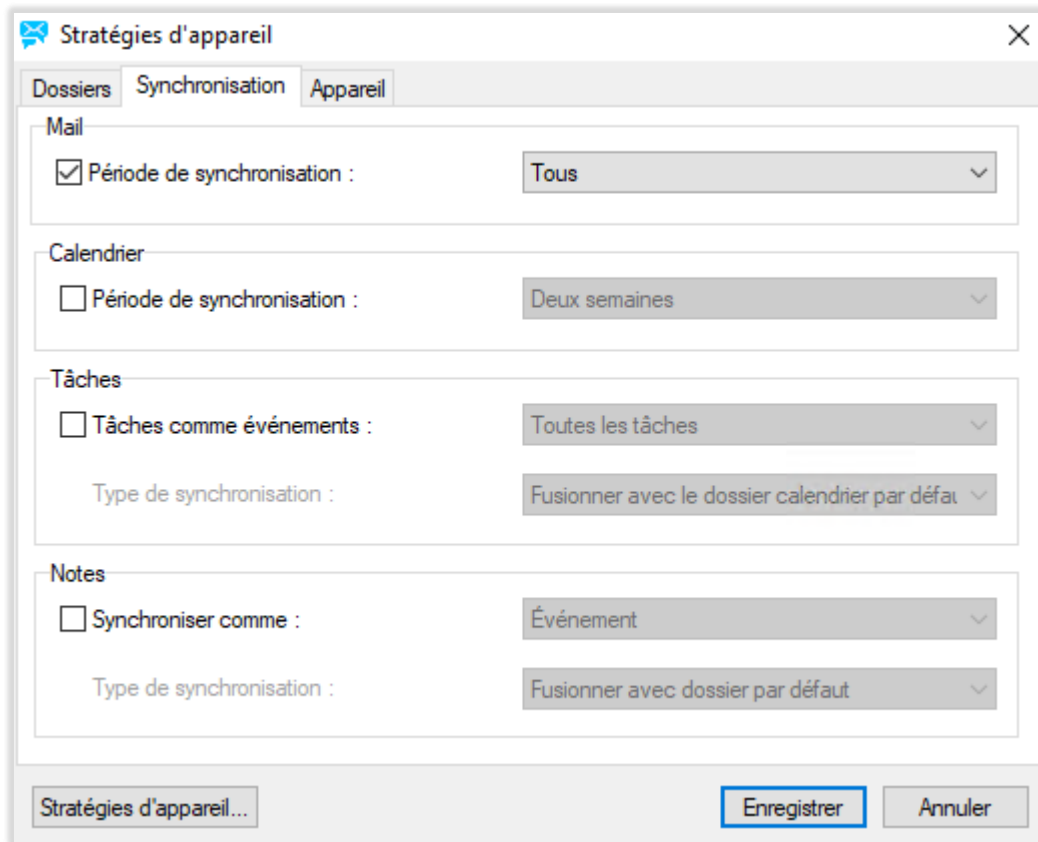
Gestion des appareils

Cette fenêtre s'obtient en double cliquant sur un appareil ou en cliquant sur le bouton "Gérer appareil..."



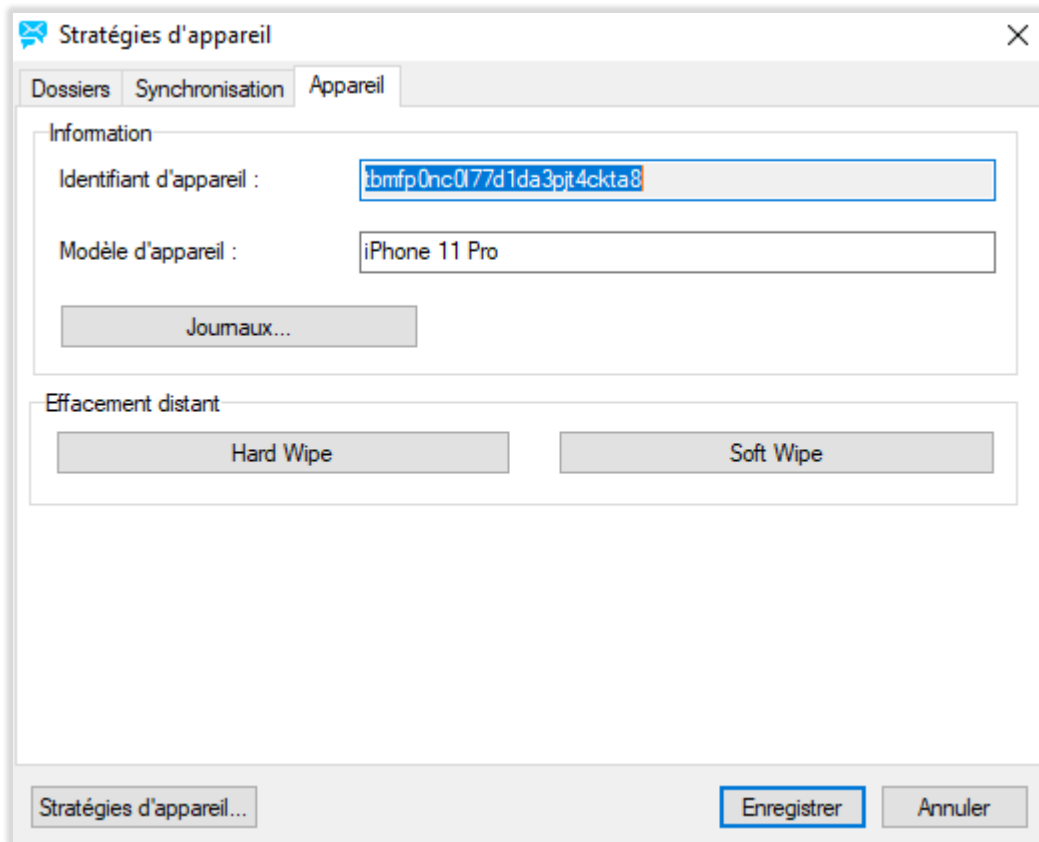
Champ	Description
Dossiers GroupWare	Sélectionner l'option désirée : <ul style="list-style-type: none"> • Uniquement les dossiers par défaut • Tous les dossiers • Tous les dossiers avec GroupWare comme email (à utiliser si les dossiers mails sont imbriqués avec les dossiers GroupWare)
Dossiers Mail	Sélectionner l'option désirée : <ul style="list-style-type: none"> • Uniquement les dossiers par défaut • Tous les dossiers
Archives	Pour synchroniser le dossier archives vers l'appareil
Dossiers publics	Pour synchroniser les dossiers publics vers l'appareil

Dossiers partagés	Pour synchroniser les dossiers partagés vers l'appareil
Stratégies d'appareil...	Détaillés au paragraphe précédent



Champ	Description
Période de synchronisation	Permet de limiter l'âge des emails qui seront synchronisés. L'appareil peut être plus restrictif. Note : certains protocoles ne supportent pas cette fonction.
Période de synchronisation	Permet de limiter l'âge des emails qui seront synchronisés. L'appareil peut être plus restrictif. Note : certains protocoles ne supportent pas cette fonction.
Tâche comme événement	Permet de synchroniser les tâches avec des appareils qui ne supportent pas nativement cette synchronisation. Sélectionner le type de tâche à synchroniser
Type de synchronisation	Permet d'indiquer dans quel calendrier ces tâches seront synchronisées (calendrier par défaut ou calendrier spécifique)
Synchroniser comme	Permet de synchroniser les notes avec des appareils qui ne supportent pas nativement cette synchronisation. Sélectionner le dossier de synchronisation (calendrier, tâches, tâches & notes)

Type de synchronisation	Permet d'indiquer dans quel dossier ces notes seront synchronisées (dossier par défaut ou dossier spécifique)
--------------------------------	---------------------------------------------------------------------------------------------------------------



Champ	Description
Identifiant de l'appareil	Ce champ montre l'identifiant de l'appareil
Modèle d'appareil	Ce champ montre le modèle de l'appareil
Journaux	Ce bouton donne accès au journal ActiveSync filtré avec l'identifiant de l'appareil
Hard Wipe	Permet de lancer l'effacement de l'appareil de type Hard Wipe L'appareil est dans ce cas réinitialisé à sa configuration usine par défaut lors de la prochaine connexion de l'appareil au serveur.
Soft Wipe	Permet de lancer l'effacement de l'appareil de type Soft Wipe Toutes les données relatives à ce compte seront effacées lors de la prochaine connexion de l'appareil au serveur.

Configuration des appareils

Attention :

Sur certains appareils, la première synchronisation peut supprimer toutes les données déjà présentes dans l'appareil (contacts, calendriers, mails...) et les remplacer par celles du compte sur le serveur.

Si vous avez des données importantes, vérifiez que vous avez une sauvegarde.

Dans d'autres cas, les données du compte seront simplement ajoutées à celles déjà existantes.

Configuration

Recherchez le menu de configuration **d'ActiveSync** sur l'appareil. Généralement, lorsque vous créez un compte, un assistant vous guide dans le processus de configuration. Si un compte ActiveSync existe déjà, vous pouvez le conserver ou supprimer (ce qui supprime toutes les données associées). Les informations nécessaires à la synchronisation de l'appareil 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 : mail.mondomaine.com)
- **Le port** associé au serveur si les ports par défaut (80 et 443) ne sont pas utilisés

Des exemples sont donnés [dans cette FAQ](#)

Configuration du compte

Pour les appareils qui utilisent la **découverte intelligente**, il suffit de 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 spécifique 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 appareils 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.
- le port associé au serveur si le port sécurisé par défaut (443) n'est pas utilisé

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

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 de l'appareil 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 et qu'une resynchronisation complète s'avère nécessaire.

Problèmes de fonctionnement

En cas de problème de fonctionnement

Version d'IceWarp

Une version 10 minimum est nécessaire.

Configuration du serveur

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

Configuration de l'appareil

Vérifiez que vous avez correctement exécuté la configuration de l'appareil telle que décrite précédemment

Vérifiez les messages d'erreurs

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

Échec de connexion au serveur - Vérifiez votre connexion sans fil. Il faut souscrire à un abonnement cellulaire avec accès aux données Internet.
Vérifiez le nom d'hôte dans la configuration ActiveSync.
Vérifiez que vous pouvez vous connecter au Client Web à partir du navigateur de l'appareil (en ajoutant /webmail/pda au nom du serveur).
Vérifiez que vous utilisez les mêmes ports que ceux du serveur Web
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.

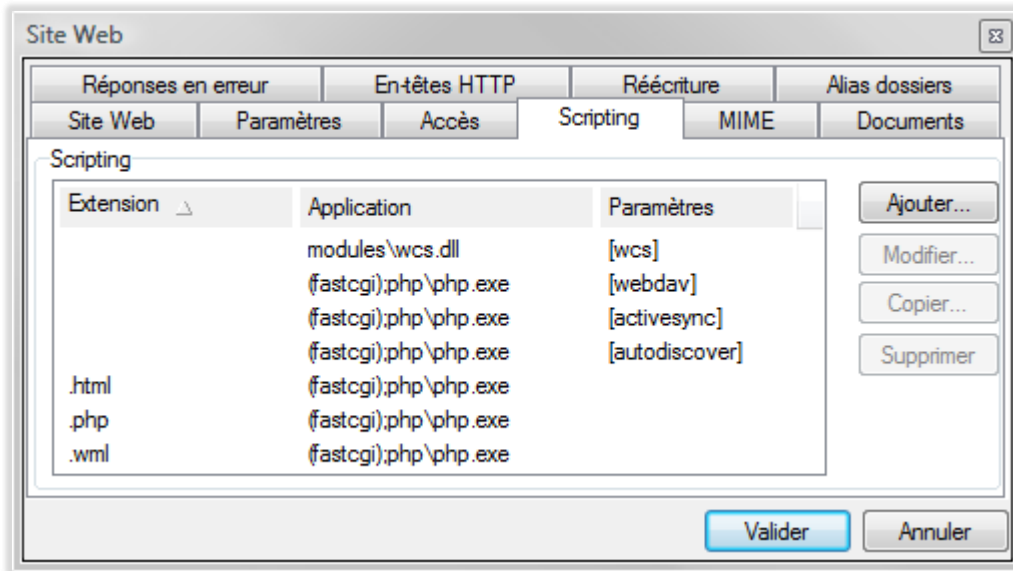
Généralement, après avoir authentifié le compte, l'appareil va faire apparaître un "Avertissement sur le certificat SSL" dans le cas d'un certificat auto signé sur le serveur et lorsque l'appareil se connecte au service de découverte automatique. Si le service n'est pas trouvé ce message va apparaître 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.

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 appareil.

Désactivez puis réactivez la synchronisation des éléments qui posent problème.

Supprimez le compte de l'utilisateur ActiveSync sur l'appareil puis recréez-le.

Utilisez l'option ActiveSync -> effacement de l'appareil pour redémarrer une synchronisation complète.

Téléchargez les dernières versions des logiciels de l'appareil et de l'application utilisée.

Consultez le manuel de l'utilisateur de l'appareil ou contactez l'aide en ligne du fournisseur de l'appareil ou de l'application.

Pour les appareils 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 appareils 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 de l'appareil 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 l'appareil en veille ou bloqué.

Sur l'appareil, désactivez tout élément de configuration qui pourrait toucher la période de pulsation de l'appareil ou mettez-la à une valeur plus faible (le 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'envoi de deux "pings" vers le serveur. Regardez les journaux de ActiveSync pour savoir au bout de combien de temps l'appareil se déconnecte et s'il se reconnecte ou non. Dans certains cas, un point d'accès WiFi mal configuré peut empêcher l'appareil 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 + liaison cellulaire.

Vérifiez les paramètres de sauvegarde de la batterie. Certains modèles coupent la connexion automatiquement lorsque le niveau batterie est faible.

Après chargement de la batterie, la reconnexion de l'appareil 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

Sur l'appareil, assurez-vous que le Push est validé.

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

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

Sur le serveur IceWarp, vérifiez que la Notification GroupWare est active dans Système -> Services -> onglet Général.

Validez le journal la Notification 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 ! L'appareil 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 l'appareil en cause.

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 l'appareil 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 de l'appareil est de 60 minutes, il sera donc ramené à 30 par le serveur) de façon à indiquer au serveur que l'appareil attend les changements sur l'adresse IP de l'expéditeur et pour conserver la session en cours. Le serveur envoie une réponse à l'appareil 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 : L'appareil 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 entraîne la synchronisation complète de certains appareils ce qui peut provoquer l'arrêt du fonctionnement du Push pendant plus d'une heure.

Une synchronisation complète signifie que toutes les données synchronisables de l'appareil 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 un cache 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 appareils actifs, désactiver le compte, enlever un appareil obsolète, faire un nettoyage à distance et régler la stratégie de sécurité.

La base de données est préconfigurée à l'installation du serveur. Par défaut, elle utilise SQLite (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 GroupWare -> ActiveSync -> onglet ActiveSync -> Paramètres BD....

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 rares, vous voudrez essayer de modifier la période de pulsation du Push. Le serveur IceWarp accepte toute période de pulsation demandé par l'appareil inférieure à 30 minutes. Normalement, l'appareil configure automatiquement une période optimale pour la pulsation. Il est possible de la régler manuellement sur certains appareils. 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 garantit une mise à jour plus fréquente de l'adresse IP d'écoute de l'appareil 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 en modifiant la variable API `c_pushserver_heartbeat`.

Aller sur la console API et indiquer la valeur en millisecondes

0 est la valeur par défaut

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 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 :

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>
```

Accès mail au GroupWare

L'accès mail au GroupWare permet d'étendre la compatibilité des appareils 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 de l'appareil 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 l'appareil comme des mails (avec ou sans le Push) avec tous les détails, catégories, participants et fichiers attachés, là où il aurait fallu installer des logiciels spécialisés sur l'appareil 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
- La procédure est complètement transparente pour tous les appareils 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 de l'appareil
- La catégorie est conservée dans le champ émetteur du message
- La synchronisation ne s'effectue que dans le sens serveur vers appareil.

Sur certains appareils, 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 appareils 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.

Durée de vie de la batterie

Pour préserver la batterie, il est préférable de ne pas valider le Push. Sur certains appareils, 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 cellulaire 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'envoi de Pings vers le serveur ce qui augmente la consommation de la batterie.

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 (Let'Encrypt, 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 appareil. Si besoin, utilisez un gestionnaire de mots de passe qui permet de définir des mots de passe forts, de faire une remise à zéro de l'appareil 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 d'appareil perdu, volé, détruit ou effacé.

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

Envisagez d'installer un anti-virus sur l'appareil.

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

- Réglez une temporisation d'inactivité suffisamment courte avant le blocage de l'appareil
- Exigez l'entrée du PIN pour le déblocage
- Validez la remise à zéro de l'appareil 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.

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, appareils, 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 appareils 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.

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 HTTPs 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 l'appareil 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 appareils 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>

Le client va alors s'authentifier par une authentification HTTPs 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 HTTPs 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>

...

</User>

...

<Account>

...

```

<Protocol>
<Type>MobileSync</Type>
<Server>https://localhost/Microsoft-Server-ActiveSync</Server>
<Name>https://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

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. 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.

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 avoir plusieurs dossiers GAL (un pour chaque dossier public) et l'utilisateur peut les consulter sur les appareils Android et iPhones 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.

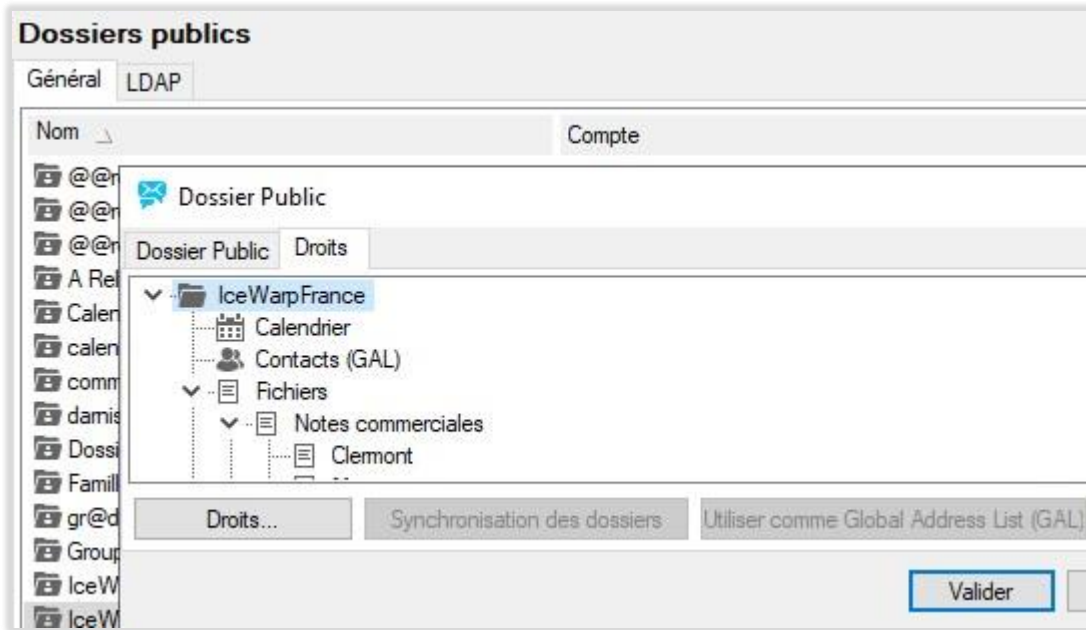
Comment créer une GAL

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.



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 toutes les requêtes incomplètes précédentes de type ajout/modification/suppression ou une réponse de modification si les informations ont changé 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 apparaîtront après la reprise normale.

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 (l'appareil 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>
    </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 -->