

Mise à jour vers FileMaker 8 :

Comment utiliser le système
de sécurité avancé

A propos de cette recommandation technique

Cette recommandation technique a pour objectif d'aider les développeurs FileMaker expérimentés à mieux comprendre le nouveau modèle de sécurité avancé de FileMaker 8.5. Elle vous permettra d'évaluer les fonctions et les avantages clés de ce nouveau modèle de sécurité ainsi que de planifier, de préparer et d'implémenter votre stratégie de migration vers FileMaker Pro 8.5. Ecrit par Steve Blackwell, membre Partenaire de l'alliance FSA (FileMaker Solutions Alliance) et président et directeur général de Management Counseling Services, ce document fait partie de toute une série de recommandations techniques rédigées par des développeurs à l'intention de développeurs, afin de les aider à migrer vers la nouvelle gamme de produits FileMaker 8.5.

Si vous recherchez des références techniques supplémentaires, reportez-vous aux manuels imprimés et électroniques ainsi qu'à l'aide en ligne fournis avec FileMaker Pro 8.5, FileMaker Server 8 et FileMaker Server 8 Advanced.

NB. : Cette recommandation technique concerne les produits FileMaker 8.x.

Introduction

Nous vivons aujourd'hui dans un monde numérique où Internet est le vecteur principal d'informations et, de plus en plus, un miroir reflétant la société dans son ensemble. Internet et ses services font partie intégrante de la vie des entreprises, quels que soient leur type et leur structure. Qu'il s'agisse d'une université offrant un accès à des bases de données de recherches scientifiques, d'une entreprise de livraison de colis offrant le suivi des expéditions, d'une organisation commerciale nationale offrant une base de données en ligne de ses membres ou d'une petite entreprise de deux salariés assurant le suivi de sa comptabilité fournisseurs et clients ou encore d'une multinationale informant les clients sur l'état de leur commande, toutes ces structures s'appuient sur des sources d'informations accessibles rapidement et mises à jour en permanence.

Nous sommes convaincus que nous pouvons réaliser en ligne tout ce que nous faisons dans le monde réel et cette conviction s'accompagne d'attentes quant au degré ou au niveau de certitude de ces actions réalisées en ligne. Or, la réalité est bien différente ; Internet est de moins en moins sécurisé et de plus en plus la cible d'attaques. D'une certaine manière, les limites de la sécurité correspondent aux limites d'Internet ; ces limites sont valables pour les systèmes FileMaker Pro® et pour les développeurs et les utilisateurs de ces produits.

Il est normal que les développeurs s'attendent à ce que la propriété intellectuelle de leurs produits logiciels soit respectée et protégée. De même, il est normal que les entreprises s'attendent à ce que leurs données personnelles soient sécurisées et protégées contre toute divulgation non autorisée, et à ce que celles-ci puissent être modifiées, amendées ou supprimées uniquement par les personnes autorisées. La sécurité est donc un point capital. La question est de savoir ce que nous cherchons à protéger et quels sont les éléments vulnérables. La sécurité des bases de données doit prendre en compte trois points spécifiques :

- la protection de la propriété intellectuelle ;
- la confidentialité des données ;
- l'intégrité des données.



La sécurité fait également partie d'un plan de continuité métier assurant la non-interruption des activités d'une entreprise dont les données sont vitales au bon fonctionnement en cas de points de défaillance multiples. Cette problématique dépasse le sujet de notre recommandation technique, il n'en demeure pas moins qu'elle est essentielle.

Cinq sujets d'intérêt pour les développeurs de solutions FileMaker Pro et pour les responsables de systèmes informatiques et de gestion de bases de données travaillant avec FileMaker Pro et FileMaker Server sont abordés dans ce document :

- une analyse rapide du modèle de sécurité de FileMaker Pro 6 et ses limites ;
- une vue d'ensemble des fonctions principales du nouveau système de sécurité de FileMaker Pro 8.5 et FileMaker Server 8 ;
- une description de plusieurs problèmes importants de gestion de sécurité résolus par le nouveau système ;
- une description de plusieurs problèmes techniques importants de développement et d'architecture rencontrés lors de la conversion de fichiers depuis des versions antérieures vers FileMaker Pro 8.5 ;
- les répercussions du nouveau système sur le travail et les activités commerciales de trois groupes métier de FileMaker Pro : *les développeurs de solutions commerciales, les développeurs consultants, les responsables de systèmes informatiques et de gestion de bases de données, notamment dans les groupes de travail des entreprises.*

Table des matières

A propos de cette recommandation technique	1
Introduction	1
Histoire passée	3
FileMaker Pro 8.5 : une nouvelle approche	3
Comptes utilisateurs et mots de passe : les informations d'authentification	3
Les jeux de privilèges	7
Les privilèges étendus	9
Planification et mise en place d'un modèle de sécurité	9
Nouvelles fonctions de gestion de la sécurité.....	10
Granularité de l'accès	10
FileMaker Server 8.....	12
Accès Web : un modèle de sécurité unifié	15
Résolution de problèmes clés de gestion de sécurité par FileMaker Pro 8.5.....	18
Gestion de compte.....	18
Trafic réseau crypté.....	20
Extraction de mot de passe.....	20
Autres problèmes résolus.....	21
Problèmes de conversion depuis des versions antérieures.....	21
Impact sur les opérations et les modèles métier pour les développeurs et les responsables de systèmes informatiques et de gestion de bases de données	23
Conclusion.....	24
A propos de l'auteur	24
Notes	25



Histoire passée

Les versions antérieures de la gamme de produits FileMaker étaient centrées sur le client et reposaient sur l'idée d'un modèle client de confiance en matière d'authentification et de reconnaissance de mot de passe². Cette approche fut responsable de problèmes significatifs qui, dans certains cas, nécessitèrent de vastes solutions de rechange ayant le plus souvent pour effet de réduire la sécurité au lieu de la renforcer. Auparavant, le trafic réseau n'était pas crypté ; il l'est aujourd'hui, ce qui représente un changement phénoménal aux retombées significatives. *En tant que développeur, nous devons tirer parti de cette opportunité unique et des avantages que ce changement nous offre.*

FileMaker Pro 8.5 : une nouvelle approche

La sécurité doit être conçue comme une problématique à part entière par les développeurs, les responsables de systèmes informatiques et de gestion de bases de données. Quel est l'intérêt d'implémenter un nouveau système si ses fonctions ne sont pas utilisées pleinement et exploitées avec pertinence ? **L'objectif premier de ce nouveau système est d'appliquer les règles et les processus nécessaires (au cas par cas) à la protection de la propriété intellectuelle ainsi qu'au respect de la confidentialité et de l'intégrité des données.**

Le système de sécurité de FileMaker Pro 8.5 possède sa propre couche dans l'architecture de la base de données, il n'est plus intégré au schéma de la base de données, où les développeurs définissent des objets comme des tables, des rubriques, des références externes et des liens. Cette séparation a des implications significatives. Les développeurs peuvent désormais attribuer à des classes d'utilisateurs (appelés ici *superutilisateurs*) la possibilité de créer, de supprimer, d'activer, de désactiver et de réinitialiser des comptes d'utilisateur et des mots de passe et ce, même lorsque les fichiers sont ouverts et hébergés par FileMaker Server 8 ou FileMaker Server 8 Advanced. Les modifications sont immédiates et sont implémentées dans tout le système. Par ailleurs, il n'est pas nécessaire que ces *superutilisateurs* aient des droits d'accès au schéma de la base de données pour gérer la sécurité ; le niveau de protection de la propriété intellectuelle est donc élevé, notamment dans le cas de développeurs de solutions commerciales.

Comptes utilisateurs et mots de passe : les informations d'authentification

Le nouveau système de sécurité FileMaker Pro 8.5 repose sur une structure de comptes : c'est par la reconnaissance d'informations d'authentification que les utilisateurs accèdent à la base de données au niveau d'accès défini par le jeu de privilèges établi par le développeur. Les informations d'authentification comprennent deux éléments : un nom de compte et un mot de passe de compte ou, un nom de groupe, dans le cas d'une authentification externe³. Une fois les informations d'authentification validées et l'utilisateur reconnu, ce dernier peut se connecter au système au niveau d'accès défini par le jeu de privilèges. La figure 1 illustre ce processus.

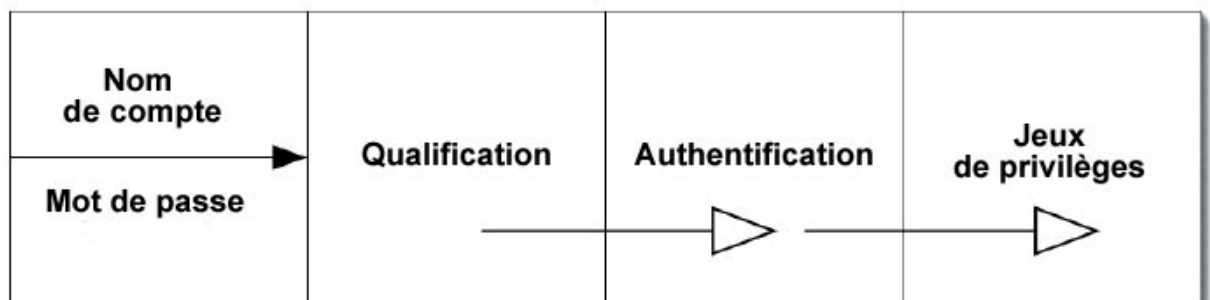


Figure 1. Le concept de base du système de sécurité.



Des règles importantes régissent l'élaboration des informations d'authentification. *Les noms de compte doivent être uniques, mais ils ne respectent pas la casse.* Cependant, lors de la création d'un compte dans plusieurs fichiers, les développeurs doivent veiller à utiliser le même nom de compte à chaque fois pour éviter toute confusion et renforcer l'organisation du système. *Les mots de passe respectent la casse, mais ils ne sont pas uniques.* Cela peut paraître source de problèmes à la première impression, ce n'est pourtant pas le cas comme nous le verrons plus loin. Ce système est totalement différent de ceux proposés dans les versions antérieures du produit. Les développeurs peuvent spécifier une longueur minimale ainsi qu'un délai d'expiration des mots de passe. Si un utilisateur oublie son mot de passe (ce qui ne manquera pas de se produire), l'administrateur doté des privilèges adéquats peut recréer le compte, réinitialiser le mot de passe, puis demander à l'utilisateur d'en choisir un nouveau.

Les développeurs définissent les comptes et mots de passe à partir du menu *Fichier*, ils peuvent également accorder des privilèges de gestion de compte aux *superutilisateurs* (voir plus loin). Sélectionnez [Fichier-Définir-Comptes et privilèges] dans le menu Fichier pour afficher une interface à onglets comme celle ci-dessous :

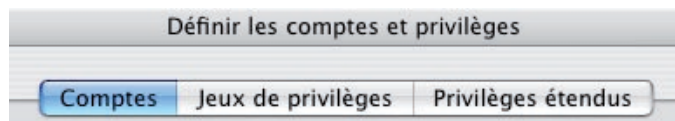


Figure 2. Onglet Définir les comptes et privilèges.

Lorsque vous sélectionnez l'onglet Comptes, une fenêtre apparaît ; celle-ci détaille les options de définition et d'authentification de compte :

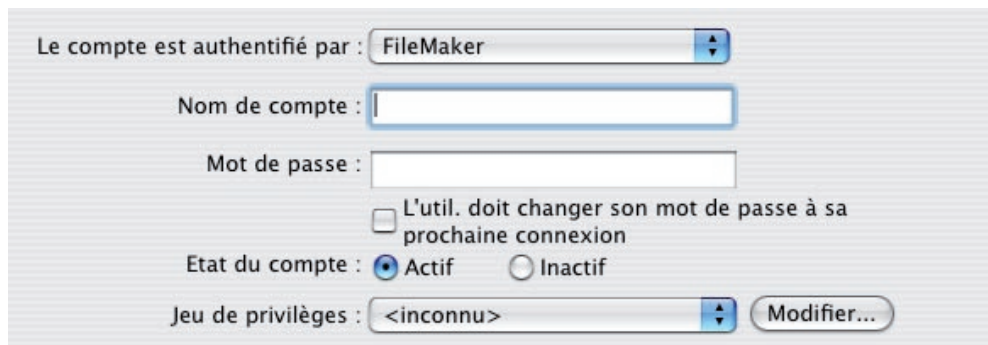


Figure 3. Boîte de dialogue Modifier compte.

Le développeur attribue un nom et un mot de passe au compte et peut exiger que l'utilisateur modifie son mot de passe à la prochaine connexion en activant la case à cocher.

D'une manière générale, la sécurité est renforcée lorsque seul l'utilisateur connaît son mot de passe, même si les administrateurs peuvent réinitialiser le mot de passe en cas d'oubli (ce qui peut se produire). Parallèlement, les noms de compte doivent être définis avec soin. Nombre d'entreprises utilisent une nomenclature standard de création de nom de compte. Par exemple : *DupontA* ou *Dupont_a* peuvent être des noms de compte standard



pour un utilisateur appelé Alain Dupont. La sécurité est ici menacée, le nom de compte étant facile à deviner. La sélection du mot de passe par l'utilisateur réduit ce risque, tout comme l'instauration de variantes dans la nomenclature des noms de compte, par exemple *DupontA##\$5*. Les mots de passe forts comportent huit caractères au minimum, à la fois alphanumériques et non alphanumériques⁴. Ils sont faciles à retenir, mais difficiles à deviner. FileMaker Pro 8.5 prend en charge des mots de passe ou des « expressions de passe » d'une longueur maximale de 100 caractères, avec les espaces. Une « expression de passe » est une *adaptation* d'une citation célèbre facile à retenir, mais difficile à deviner, comme :

Chassez le naturiste, il revient toujours au bungalow

Lorsqu'un développeur crée un nouveau fichier FileMaker Pro 8.5 pour la première fois, l'application crée un compte par défaut appelé *Admin* sans mot de passe et l'attribue au jeu de privilèges [Accès intégral] comme illustré dans la figure 4. FileMaker Pro 8.5 définit également une connexion automatique⁵ à partir du nom de compte *Admin* et d'un mot de passe vide. Le développeur peut ainsi travailler sur le fichier. Il est cependant recommandé de renommer le compte par défaut dès la première utilisation et de lui attribuer un mot de passe ; dans le cas contraire, il reste inchangé et est très facile à trouver, ce qui entraîne l'accès au fichier. Il est fortement conseillé de conserver les informations d'authentification liées aux jeux de privilèges [Accès intégral] ; le mot de passe n'est en effet pas récupérable, même par FileMaker Inc., en cas de perte ou d'oubli.

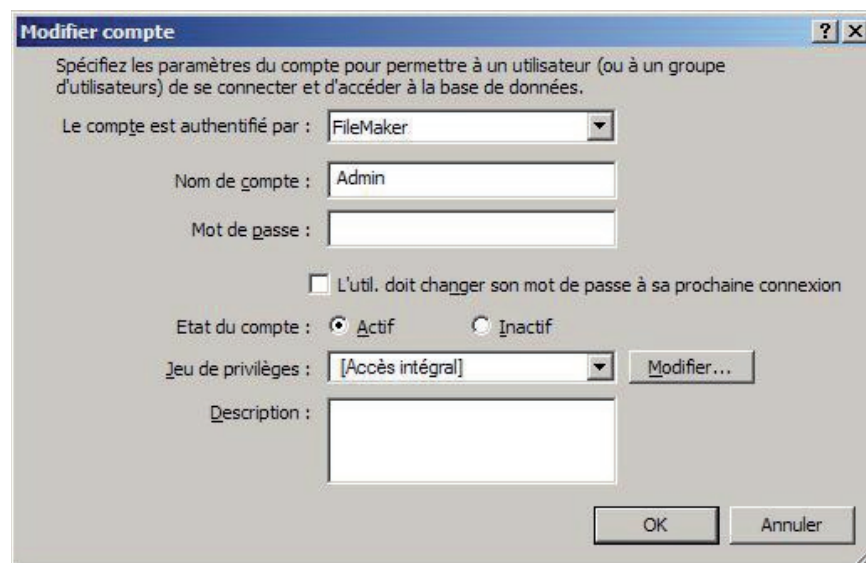


Figure 4. Le compte *Admin* par défaut avec les privilèges [Accès intégral].

Le développeur sélectionne également la méthode d'authentification dans la boîte de dialogue *Modifier compte* : *FileMaker* ou *Serveur Externe*. Dans le deuxième cas, l'écran est légèrement différent comme illustré dans la figure 5.



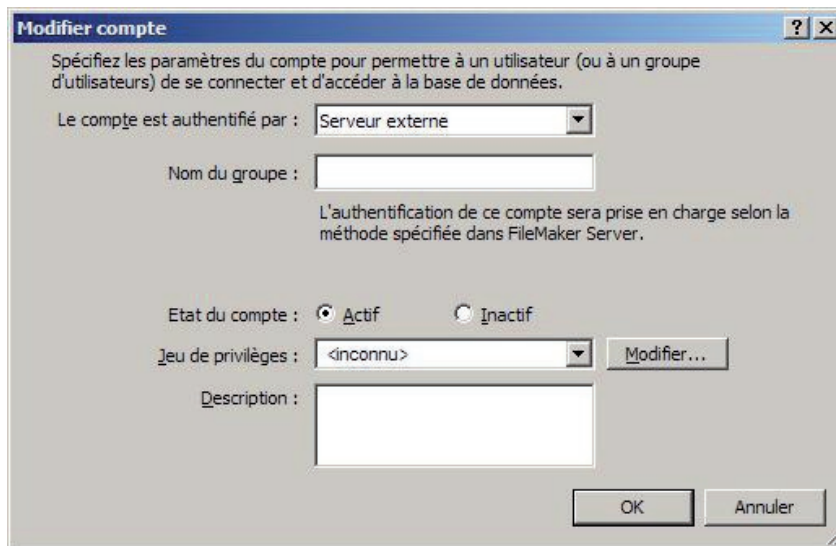


Figure 5. La boîte de dialogue Modifier compte avec les options d'authentification externe.

Remarquez que Nom de compte est devenu Nom du groupe. Vous devez y saisir le nom d'un groupe du domaine externe⁶ : FileMaker Server 8 gère alors le processus d'authentification en externe. Les points suivants relatifs à ces options de définition et d'authentification de compte sont à prendre en compte :

1. Tous les fichiers doivent avoir au minimum un compte [Accès intégral] authentifié en interne (par FileMaker Pro)⁷.
2. Il est fortement déconseillé d'authentifier un compte avec des privilèges [Accès intégral] par des méthodes externes. Dans le cas de l'obtention d'une copie physique du fichier, le système de domaine pourrait être recréé et le compte de domaine contrefait, ce qui garantirait un accès intégral aux fichiers.
3. En termes de sécurité, l'attribution de noms de compte doit être réservée à des *utilisateurs individuels*. **Les informations d'authentification ne doivent pas être partagées ou divulguées.** Le caractère individuel et personnel des informations est au cœur du système FileMaker, garantissant ainsi les trois piliers de la sécurité : la protection de la propriété intellectuelle, la confidentialité des données et l'intégrité de celles-ci.

Quand faut-il utiliser une méthode d'authentification plutôt qu'une autre ? Dans certains cas, les développeurs utiliseront une authentification FileMaker interne, car la solution sera déployée dans une entreprise dépourvue de structure de domaine. Cependant, dans la majeure partie des cas, il est fort probable que les développeurs consultants et les développeurs en interne opteront pour la méthode d'authentification externe afin de tirer parti des actifs informatiques existants et de normaliser la gestion de comptes et de solutions multiples. Les informations d'authentification de domaine de l'utilisateur sont alors utilisées pour accorder l'accès à la base de données FileMaker Pro à un niveau d'accès donné. Un fichier peut être doté de comptes authentifiés en interne et en externe, l'administrateur choisit alors l'option à utiliser dans FileMaker Server 8 : *Comptes FileMaker uniquement* ou *Comptes FileMaker et serveur externe* (voir plus loin).



Grâce à l'option d'authentification externe, FileMaker Pro 8.5 et FileMaker Server 8 prennent en charge des connexions de source unique, parfois appelées connexion d'authentification universelle ou connexion unique (ou connexion unique (SSO - Single Sign-On)). Il s'agit là d'une technique couramment employée pour la gestion de systèmes informatiques et de réseaux. A première vue, cette méthode semble simplifier les activités de gestion des informations d'authentification de l'utilisateur, car ce dernier n'a besoin de se souvenir que d'un jeu d'informations pour accéder aux actifs numériques et aux actifs réseau. C'est en partie vrai, mais le fait est que cette méthode entraîne un transfert de la sécurité de la base de données hors des limites de FileMaker Pro. Il est donc conseillé de se documenter sur l'authentification et la sécurité réseau de manière générale⁸.

Jeux de privilèges

Une fois qu'un développeur a créé un nouveau fichier FileMaker Pro 8.5, il peut affecter des comptes à l'un des jeux de privilèges par défaut. Il existe deux types de jeux de privilèges : [Accès intégral] et tous les autres jeux qui sont *subalternes*. Ces jeux de privilèges subalternes, qu'ils existent par défaut ou aient été créés, sont dotés de restrictions intrinsèques. Il est **impossible** de créer un jeu de privilèges [Accès intégral] ; seul celui par défaut est disponible. Il existe deux jeux de privilèges par défaut autre que [Accès intégral], tous deux subalternes : [Saisie de données uniquement] et [Accès en lecture seule] . Il est conseillé d'examiner avec attention les éléments présents dans chacun de ces jeux de privilèges subalternes par défaut avant de les affecter à des comptes. Dans bien des cas, leur nom peut être trompeur et ils peuvent contenir un niveau d'accès différent de celui escompté par le développeur. C'est pourquoi il est possible de choisir un compte spécifique pour « Saisie de données uniquement » et pour « Accès en lecture seule ».

La création de jeux de privilèges subalternes personnalisés est essentielle ; c'est ainsi que toute la richesse et la souplesse du nouveau système de sécurité seront vraiment mises à jour. Les jeux de privilèges sont au cœur du modèle d'application de la sécurité de FileMaker Pro 8.5 : ils définissent les actions autorisées et les droits d'un utilisateur pour un fichier donné ainsi que pour toutes les tables contenues dans ce fichier.

Dans la boîte de dialogue *Définir les comptes et privilèges* (figure 6), cliquez sur le deuxième onglet Jeux de privilèges pour afficher la fenêtre de création de jeux de privilèges subalternes personnalisés, similaire à celle de la figure 7.

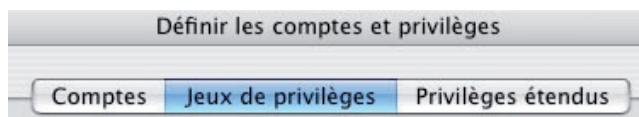


Figure 6. Fenêtre *Définir les comptes et privilèges*



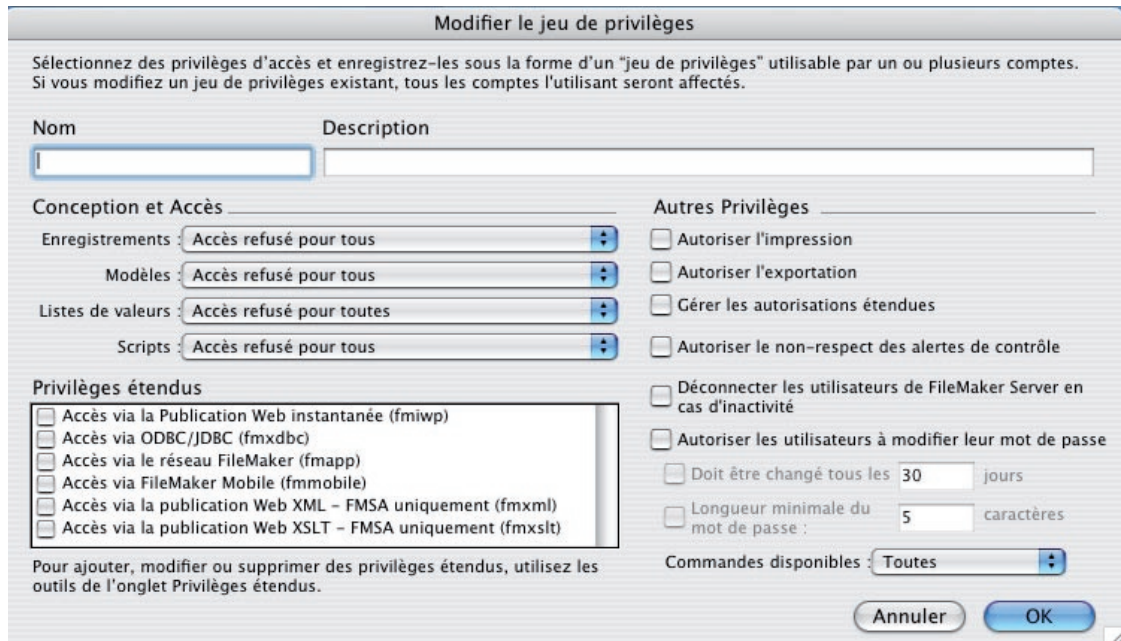


Figure 7. Fenêtre Modifier le jeu de privilèges.

Notez que la plupart des options ne sont *pas activées* par défaut. Il s'agit là d'un changement considérable par rapport aux versions antérieures où la solution était ouverte ; le développeur devait désactiver l'accès objet par objet. FileMaker Pro 8.5 s'appuie sur un modèle d'accès fermé par défaut où les autorisations doivent spécifiquement être attribuées à une large palette d'objets et de fonctions.

Chaque compte est affecté à *un seul et unique* jeu de privilèges, mais un jeu de privilèges donné peut avoir plusieurs comptes qui lui sont affectés. Il s'agit là aussi d'un changement important par rapport aux versions antérieures où les mots de passe pouvaient être attribués à plusieurs groupes. La fenêtre Jeu de privilèges comporte trois zones différentes : *Conception et accès*, *Privilèges étendus* et *Autres privilèges*.

Reportez-vous à la partie relative à la granularité de l'accès pour de plus amples informations sur ce sujet. Cette fenêtre est également dotée d'une nouvelle zone de texte appelée Description pour la saisie d'un commentaire ou d'une description de l'objet du jeu de privilèges. Cette fonction est fort utile pour la gestion d'architecture et pour la documentation technique de solutions.



Privilèges étendus



Figure 8. Onglet Privilèges étendus.

La figure 8 montre le dernier onglet des options Définir les comptes et privilèges. Une fenêtre apparaît lorsque vous cliquez sur cet onglet ; les utilisateurs peuvent y être autorisés à affecter des privilèges étendus à divers jeux de privilèges et par extension, aux comptes liés au jeu de privilèges en question. La plupart de ces privilèges concernent des options de connexion réseau, comme l'accès depuis FileMaker Server, la publication Web instantanée et la publication Web personnalisée via le nouveau moteur de publication Web de FileMaker Server 8 Advanced, mais aussi des options de connexion ODBC/JDBC à la base de données et FileMaker Mobile. En outre, il est possible de définir des privilèges étendus personnalisés pour une utilisation avec différents modules externes ou internes.

Planification et mise en place d'un modèle de sécurité

Les développeurs doivent envisager la planification de la sécurité d'une toute autre manière avec le nouveau modèle en la matière proposé par FileMaker Pro 8.5 ; tout est question de nuance et l'expérience pratique a beaucoup plus de valeur que toute recommandation en matière de bonnes pratiques.

Pendant, d'une manière générale, il est conseillé de créer plusieurs jeux de privilèges subalternes personnalisés une fois les spécifications de la solution établies, ainsi que d'attribuer à chacun de ces jeux un nom de compte et un mot de passe facilement identifiables pour la phase de test pendant le développement⁹. Ainsi, le jeu de privilèges est doté d'une plus grande souplesse et l'attribution de privilèges aux objets peut se faire à un niveau granulaire plus fin si nécessaire.

Pour les solutions plus complexes (mais cela s'applique aussi aux solutions simples), il est utile d'insérer une section traitant explicitement des privilèges d'accès dans les spécifications de conception. La définition de ces jeux de privilèges peut s'avérer éprouvante : quelle est la planification la plus adaptée à une utilisation efficace du nouveau système de sécurité ? Il existe plusieurs processus distincts et bien définis de gestion d'accès :

- contrôle d'accès obligatoire ;
- contrôle d'accès discrétionnaire (largement utilisé dans les fichiers FileMaker Pro 6) ;
- contrôle d'accès basé sur des règles ;
- contrôle d'accès basé sur des rôles.

Dans cette dernière approche, les développeurs élaborent un jeu de privilèges subalterne personnalisé pour chaque rôle identifié dans la base de données, puis lui affectent autant de comptes qu'il existe d'utilisateurs remplissant ce rôle¹⁰.



Nouvelles fonctions de gestion de la sécurité

FileMaker Pro 8.5 offre de nouvelles fonctions de gestion de sécurité, capables de renvoyer des informations sur le compte utilisé pour l'accès au fichier. Il s'agit de fonctions d'obtention, remplaçant les fonctions d'état, notamment `OBTENIR(NOMCOMPTE)`¹¹, `OBTENIR(NOMPRIVILEGES)` et `OBTENIR(PRIVILEGESETENDUS)`. La fonction `OBTENIR(NOMUTILISATEUR)` existe toujours, mais son intérêt est désormais limité¹². Enfin, certaines fonctions réseau et UC sont également pertinentes en matière de sécurité, notamment `OBTENIR(ADRESSENICSYSTEME)` et `Obtenir(ADRESSEIPSYSTEME)`. Les résultats pertinents renvoyés par ces fonctions sont les scripts, les calculs, les tests d'Accès aux enregistrements et autres résultats de même nature, qui aident à identifier le compte et à créer les conditions correspondant à l'identification.

Granularité de l'accès

La *granularité* correspond au niveau de contrôle d'accès discret et différencié que le système de sécurité attribue à toute une palette d'objets et de fonctions FileMaker Pro :

Objets

Table
Création de script ScriptMaker™
Accès aux scripts ScriptMaker
Création de listes de valeurs
Accès aux listes de valeurs
Création de modèles
Accès aux modèles
Enregistrement
Rubrique

Fonctions

Impression
Exportation
Gestion de son mot de passe
Options de partage de base de données, notamment réseau, ODBC/JDBC, publication Web instantanée, publication Web personnalisée et FileMaker Mobile
Déconnexion en période d'inactivité
Accès aux schémas dans des conditions encadrées
Gestion de compte
Manipulation API externe
Gestion des privilèges étendus

Il faut faire une distinction entre la *gestion* de privilèges étendus et les privilèges étendus en eux-mêmes. La gestion correspond à la capacité d'activer ou de désactiver les privilèges étendus, de créer ou de supprimer des privilèges personnalisés et enfin d'attribuer ou d'ôter des privilèges étendus à des jeux de privilèges spécifiques (voir plus loin pour de plus amples informations sur les privilèges étendus).



Pour les développeurs qui ne souhaitent pas personnaliser les paramètres à un niveau élevé de granularité, FileMaker Pro 8.5 (tout comme les versions antérieures) offre toute une gamme de paramètres standard de sécurité qui permet une affectation rapide des options d'accessibilité pour créer des jeux de privilèges subalternes personnalisés. La figure 9 en est un exemple.

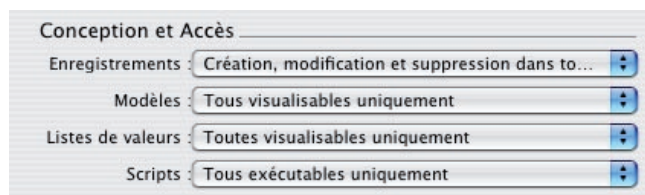


Figure 9. Options d'accès standard.

La granularité est un concept très important ; c'est par son utilisation extensive que le développeur contrôle l'accès aux objets et aux fonctions du fichier et ainsi, garantit le respect des trois piliers de la sécurité : la protection de la propriété intellectuelle, la confidentialité des données et l'intégrité de celles-ci. Il existe au moins quatre niveaux de contrôle pouvant être appliqués objet par objet ou à une catégorie entière. Ce processus est effectué jeu de privilège par jeu de privilège pour tout jeu de privilèges subalterne personnalisé afin d'améliorer la granularité du contrôle d'accès. Les différents niveaux sont les suivants :

- *Création*, hormis pour les tables, les rubriques et les liens (ceux-ci peuvent cependant être créés dans un contexte bien précis)¹³ ;
- *Modification*, comprend également la suppression ;
- *Lecture seule*, ou *Tous exécutables* seulement dans le cas de scripts
- *Accès refusé*.

L'application de ces contrôles aux objets créés par les développeurs peut se faire de manière sélective, par opposition aux objets créés par la suite par les administrateurs et les utilisateurs finaux. **Ce qui signifie qu'un administrateur, voire même un utilisateur final, peut se voir attribuer la possibilité de créer des modèles, des scripts et des listes de valeur sans pour autant pouvoir modifier ceux qui existent déjà.**

Les implications de cette distinction sont significatives : d'une part, la propriété intellectuelle des produits du développeur est ainsi protégée par une telle granularité d'accès, notamment les solutions commerciales, d'autre part, les processus métier propriétaires sont protégés de toute interruption, pendant que les administrateurs ont la possibilité de personnaliser des fonctionnalités supplémentaires.

Les scripts disposent de fonctionnalités spéciales correspondant à leur rôle élémentaire dans le processus FileMaker Pro. Les développeurs peuvent définir un script spécifique comme *Modifiable* pour chaque jeu de privilèges subalterne personnalisé, ce qui signifie que l'utilisateur a la possibilité de le modifier. Le script peut également être défini comme *Exécutable uniquement* ; l'utilisateur a alors accès au script, mais pas à ses différentes étapes logiques et individuelles et ne peut pas le modifier. Enfin, le script peut être défini comme *Accès refusé* ;



l'utilisateur n'y a pas accès et ne sait pas qu'il existe : il n'apparaît pas dans la liste de scripts, même lorsque ScriptMaker™ est ouvert. Un même utilisateur peut créer de nouveaux scripts, sans pour autant voir ceux définis comme *Accès refusé* dans le jeu de privilèges auquel est affecté son compte.

La figure 10 montre les options de scripts et celle *Autorisations d'accès personnalisées*, qui permet une différenciation des options d'accès pour chaque script. FileMaker Pro 8.5 possède des niveaux de granularité similaires pour la plupart des objets, comme indiqué dans le tableau suivant.

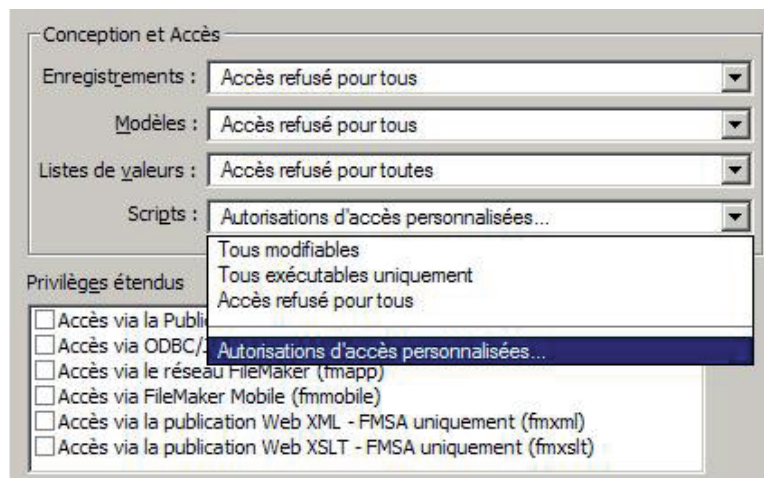


Figure 10. Options d'accessibilité des scripts de niveau granulaire élevé.

FileMaker Server 8

FileMaker Server 8 et FileMaker Server 8 Advanced représentent des avancées majeures en termes de sécurité, notamment sur trois points essentiels : l'authentification, la visibilité des fichiers et le cryptage des données.

Les versions Macintosh OS X et Windows 2000 Server/Windows 2003 Server de FileMaker Server 8 intègrent des critères d'authentification de sécurité pour l'accès au démon ou au service. Vous trouverez de plus amples informations sur ces éléments dans une autre recommandation technique sur FileMaker Server 8. Globalement, il est possible de configurer une authentification au niveau de la connexion pour l'accès et l'administration. Le contrôle de la sécurité physique de l'unité centrale sur laquelle est exécutée FileMaker Server 8 ainsi que de celle des fichiers hébergés est vital. Pour améliorer la sécurité, il est conseillé de prendre quelques précautions, comme désactiver le partage de fichiers au niveau du système d'exploitation, placer l'unité centrale dans un environnement fermé et sécurisé et conserver toutes les copies de sauvegarde des fichiers dans un lieu sûr. Par ailleurs, FileMaker Server 8 est doté de fonctions de connexion étendues¹⁴, aussi bien au serveur qu'aux fichiers hébergés, ce qui contribue au contrôle des processus et de l'accès.

Les figures 11A et 11B illustrent les panneaux de sécurité Macintosh OS X et Windows 2000 Server/2003 Server pour FileMaker Server 8.



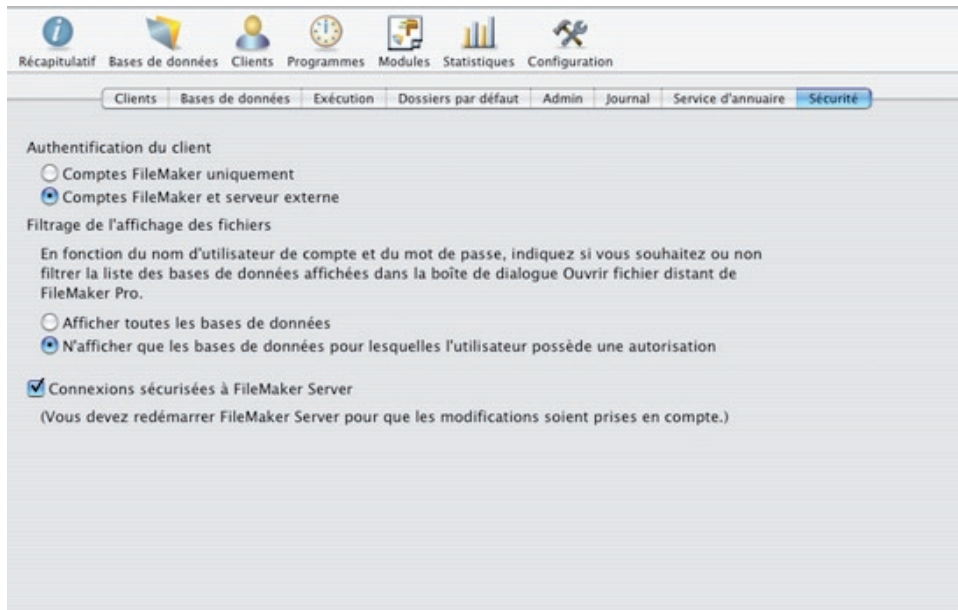


Figure 11A. Onglet de gestion de la sécurité de FileMaker Server 8 sous Macintosh OS X.

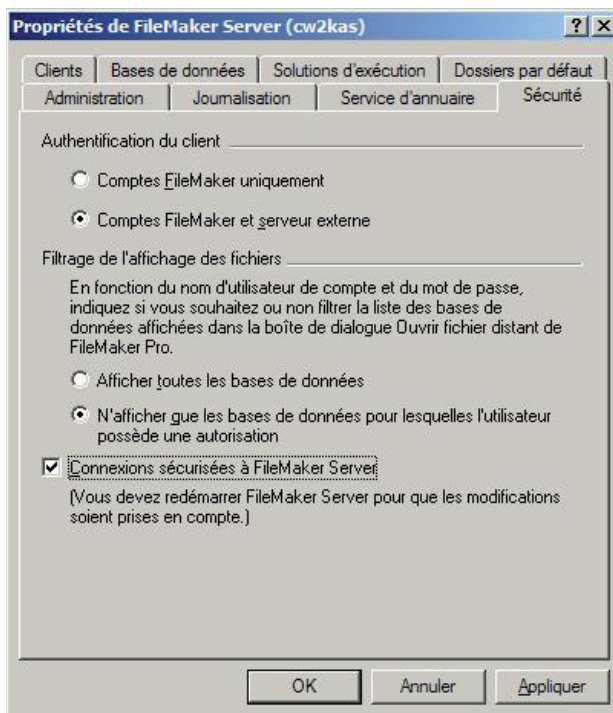


Figure 11B. Onglet de gestion de la sécurité de FileMaker Server 8 sous Windows 2003 Server.



Comme nous l'avons vu précédemment, FileMaker Pro 8.5 gère l'authentification externe des comptes. Remarquez l'option *Authentification du client*. Que ce soit avec une version Macintosh ou avec une version Windows, l'administrateur du serveur peut sélectionner *Comptes FileMaker uniquement* ou *Comptes FileMaker et serveur externe*.

Les développeurs et les responsables de systèmes informatiques et de gestion de bases de données doivent tenir compte de plusieurs considérations d'architecture et de déploiement lors de l'utilisation d'une authentification externe. Premier point, l'option *Comptes FileMaker uniquement* désactive les comptes authentifiés en externe dans un fichier de base de données FileMaker Pro 8.5 spécifique.

Second point, dans des domaines d'entreprise, les utilisateurs appartiennent généralement à plusieurs groupes de domaine¹⁵, d'où la question suivante qui se pose : par rapport à quel groupe l'utilisateur doit-il être authentifié lors de l'accès aux fichiers de la base de données ? L'utilisatrice *Sara Jolly* est membre du groupe Marketing, du groupe Developer et du groupe FSA Partner. Chacun de ces groupes est doté d'un compte dans le fichier de la base de données et chaque compte possède des privilèges différents en fonction du jeu de privilèges auquel il est affecté. Comment l'accès est-il déterminé ? Le développeur doit sélectionner l'ordre d'authentification dans l'onglet *Comptes* de la section *Définir les comptes et privilèges* de la base de données. Le **premier** compte correspondant trouvé dans l'ordre d'authentification est celui utilisé pour déterminer les privilèges. La figure 12 illustre ce concept : *Sara Jolly* se connectera avec le compte *FSA Partner* et le jeu de privilèges *Superuser* dans le cas d'une authentification externe. Les développeurs ainsi que les responsables de systèmes informatiques et de gestion de bases de données doivent s'assurer que les niveaux d'accès attendus sont respectés dans le cas de membres appartenant à plusieurs groupes. De tels utilisateurs peuvent bien évidemment avoir accès aux fichiers avec un compte authentifié en interne si nécessaire.

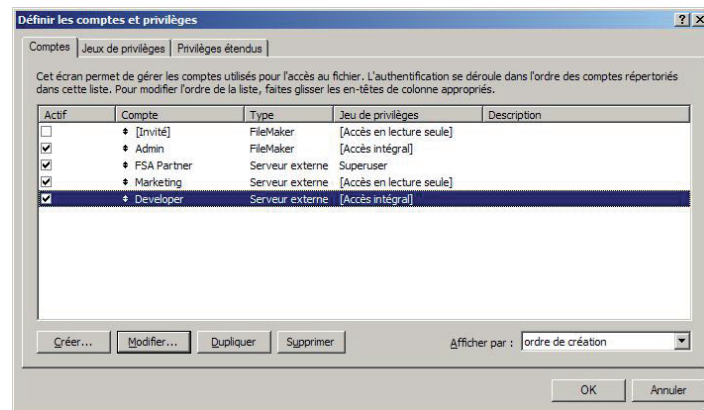


Figure 12. L'ordre d'authentification détermine le compte et le jeu de privilèges correspondant sélectionné à partir d'une authentification externe lorsque l'utilisateur appartient à plusieurs groupes de domaine.

Reportez-vous à nouveau aux figures 11A et 11B pour la seconde option, Connexions sécurisées à FileMaker Server, qui peut être soit activée, soit désactivée. Lorsqu'elle est activée, les flux de données entre les clients FileMaker Pro 8.5 et FileMaker Server 8 sont cryptés, ainsi que ceux entre FileMaker Server 8 et le nouveau moteur de publication Web, que ce soit pour la publication Web instantanée ou personnalisée. Vous trouverez de plus amples informations sur l'impact de cette option sur l'accès des comptes Web dans la section suivante sur le modèle unifié.



La troisième option FileMaker Server 8 présentée sur les figures 11A et 11B concerne l'affichage des noms de fichier dans l'option de menu Ouvrir à distance [Fichier-Ouvrir à distance...] de FileMaker Pro 8.5. Si l'option Afficher toutes les bases de données est sélectionnée, toutes les bases de données apparaissent. Si l'option N'afficher que les bases de données pour lesquelles l'utilisateur possède une autorisation est sélectionnée, l'utilisateur doit d'abord être doté d'un compte authentifié dans la base de données pour pouvoir y accéder.

Lorsque cette option de filtrage ou de visibilité est activée et qu'un utilisateur tente de se connecter au serveur, FileMaker Pro 8.5 recherche les informations de compte en mémoire de cet utilisateur. Pour cela, le gestionnaire de mots de passe du Trousseau d'accès (Keychain) sous Macintosh OS X ou les informations d'authentification de l'utilisateur sous Windows 2000 Professionnel et Windows XP Professionnel sont utilisés. Si la recherche ne donne aucun résultat, une boîte de dialogue modale apparaît, demandant à l'utilisateur de saisir ses informations d'authentification (un nom de compte et un mot de passe) pour visualiser les bases de données hébergées par le serveur. Il est possible de faire apparaître cette boîte de dialogue en appuyant sur la touche OPTION sous Macintosh OS X ou la touche MAJ sous Windows 2000 Professionnel ou Windows XP Professionnel et en la maintenant enfoncée lorsque l'utilisateur sélectionne le nom de serveur dans l'élément de menu Ouvrir à distance... Si les informations saisies sont incorrectes, une seconde boîte de dialogue modale apparaît, demandant à l'utilisateur de se connecter au serveur avec des informations d'authentification différentes.

Accès Web : un modèle de sécurité unifié

Les fonctionnalités de sécurité de FileMaker Pro 8.5 offrent un modèle unifié aux utilisateurs accédant aux bases de données via des navigateurs Web. Les développeurs peuvent permettre aux utilisateurs disposant d'un accès via le Web de créer leur propre compte et de l'intégrer facilement dans la base de données, ce qui est fort pratique, notamment pour les systèmes d'inscription en ligne. Des jeux de privilèges subalternes personnalisés peuvent être affectés à des comptes d'utilisateur Web, comme à tout autre compte. Les privilèges d'un jeu donné sont appliqués aux utilisateurs Web que ce soit pour la publication Web instantanée ou personnalisée. Par ailleurs, si un utilisateur connecté à un réseau local a reçu l'autorisation d'accéder à un fichier du Web via un navigateur, les privilèges du client FileMaker Pro sur réseau local s'appliquent à cet accès Web. Un ensemble exhaustif de règles d'accès peut ainsi être appliqué compte par compte et table par table. Dernier point, l'option de filtrage ou de visibilité est également valable pour un accès Web.

Les administrateurs ont la possibilité de gérer des comptes dans des fichiers FileMaker Pro sur réseaux local et étendu à partir d'interfaces Web si les autorisations ont été correctement configurées. Cette fonction soulève cependant des questions décisionnelles et réglementaires pour l'entreprise.

Les utilisateurs Web peuvent tirer parti des options de cryptage de FileMaker Server 8. Lorsque le cryptage est activé, un canal crypté entre les clients FileMaker Server 8 et FileMaker Pro 8.5 ainsi qu'un canal vers le moteur de publication Web sont créés. Reportez-vous aux recommandations techniques relatives à FileMaker Server et à la publication Web FileMaker pour de plus amples informations sur la configuration du moteur de publication Web. Apache et Microsoft IIS prennent en charge les connexions SSL depuis des navigateurs Web modernes. Il reste donc à assurer la protection entre le moteur de publication Web et Apache ou IIS pour couvrir la totalité du canal de données. Différentes approches sont disponibles pour assurer la protection de cette dernière partie¹⁶. Pour que FileMaker Server 8 et FileMaker Server 8 Advanced autorisent les connexions Web, le serveur doit avoir reçu l'instruction d'accepter de telles connexions et disposer de la clé d'installation garantissant ce privilège.



Reportez-vous aux recommandations techniques sur la publication Web FileMaker 8 et sur FileMaker Server 8. Il en va de même pour les connexions ODBC/JDBC ; avant que de telles connexions puissent être autorisées, celles-ci doivent être activées dans l'onglet *Clients* de FileMaker Server 8 et de FileMaker Server 8 Advanced. Point supplémentaire pour la publication Web instantanée, personnalisée et les connexions ODBC/JDBC, les développeurs, ou dans certains cas les *superutilisateurs*, doivent activer le privilège étendu approprié du fichier à partager. Il est possible de configurer ces privilèges étendus à partir d'un jeu de privilèges individuel.

Ci-dessous une autre partie de la fenêtre Modifier le jeu de privilèges déjà illustrée à la figure 7. Les six privilèges étendus par défaut sont représentés dans la figure 13.

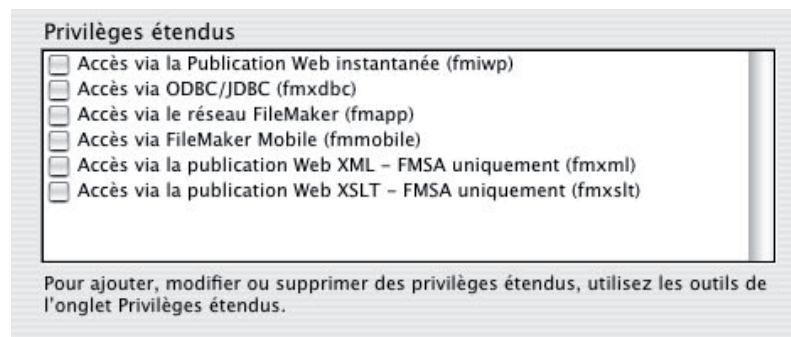


Figure 13. Privilèges étendus par défaut

Les développeurs doivent vérifier les options de privilèges étendus pour la publication Web instantanée (mot-clé *fmiwp*) et pour ODBC/JDBC (mot-clé *fmxdbc*), notamment en matière d'attribution du jeu de privilèges [Accès intégral]. Tout compte auquel ce jeu de privilèges est affecté peut alors accéder aux fichiers à condition qu'ils soient hébergés sur FileMaker Server 8. Une chaîne complète de contrôle de la sécurité doit être suivie :

- activation des privilèges étendus pour un jeu de privilège donné ;
- reconnaissance des informations d'authentification de l'utilisateur (nom de compte et mot de passe) pour le compte auquel ce jeu de privilèges est affecté ;
- vérification de la clé d'installation de FileMaker Server et de sa configuration pour l'autorisation des connexions publication Web instantanée, publication Web personnalisée et ODBC/JDBC.

Si l'un de ces éléments (par exemple, les privilèges étendus) n'est pas activé, il est impossible d'accéder au fichier avec un compte auquel ce jeu de privilèges est affecté, même si le fichier est hébergé par FileMaker Server. Pour attribuer des droits d'accès à un fichier via la publication Web personnalisée, le développeur doit sélectionner deux privilèges étendus personnalisés à l'aide des mots-clés *fmxml* et *fmxslt*, selon le type d'accès à la publication Web personnalisée souhaité¹⁷. La figure 14 montre ces privilèges ainsi que ceux de la publication Web instantanée lorsqu'ils sont activés.



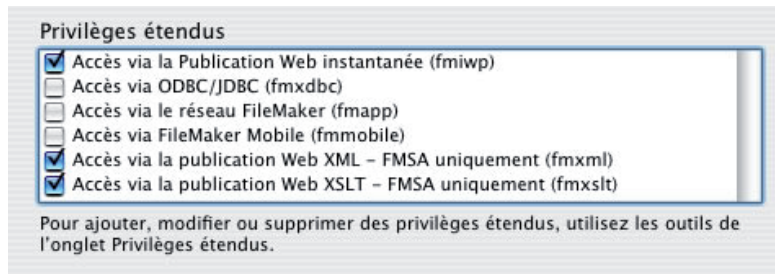


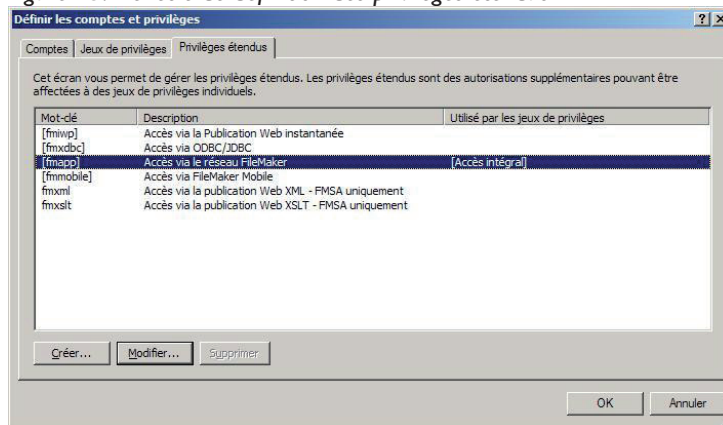
Figure 14. Privilèges étendus de la publication Web personnalisée et de la publication Web instantanée.



La figure 8 illustre l'onglet Privileges étendus. Ci-dessus pour référence:

En cliquant sur cet onglet, une fenêtre similaire à celle de la figure 15 apparaît. A partir de cette fenêtre, le développeur ou le *superutilisateur* doté des privilèges appropriés peut définir de nouveaux privilèges étendus personnalisés et les affecter à divers jeux de privilèges. Ces privilèges étendus seront alors disponibles pour les comptes auxquels ces jeux de privilèges sont affectés. La figure 7 indique où sélectionner cette option pour obtenir les droits de gestion des privilèges étendus pour un jeu de privilèges subalterne personnalisé : activez l'option *Gérer les autorisations étendues* de la zone *Autres privilèges*. Tout utilisateur doté d'un compte authentifié auquel ce jeu de privilèges est affecté peut gérer les privilèges étendus.

Figure 15. Fenêtre de définition des privilèges étendus



Lorsque le développeur ou le *superutilisateur* clique sur le bouton *Nouveau...* ou le bouton *Edition...*, une boîte de dialogue similaire à celle de la figure 16 apparaît. De nouveaux privilèges étendus personnalisés peuvent être définis et affectés à des comptes dans cette boîte de dialogue. Notez que l'attribution de l'accès à cette fonction à un utilisateur permet à ce dernier d'ôter les privilèges étendus de tous les comptes du fichier, notamment de ceux associés aux jeux de privilèges [Accès intégral]. Il est évident que dans certains cas, ce comportement n'est pas souhaitable ; il faut donc que l'attribution des droits de gestion des privilèges étendus soit le résultat d'une



décision bien réfléchiée. En effet, il est fort probable que l'attribution de ces droits sera une nécessité dans les déploiements d'entreprise, notamment aux administrateurs et aux *superutilisateurs*.

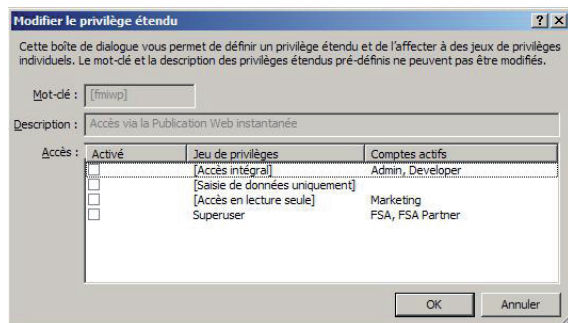


Figure 16. Modification et attribution des privilèges étendus.

Résolution de problèmes clés de gestion de sécurité par FileMaker Pro 8.5

Le nouveau système de sécurité FileMaker Pro 8.5 apporte des améliorations aux fonctions des versions antérieures des produits, les principales étant la gestion de l'accès, l'interception du trafic réseau, la granularité du contrôle des objets et des fonctions, l'extraction de mots de passe et la manipulation des fichiers FileMaker Pro via un éditeur de texte.

Gestion de compte

Dans les versions antérieures, la gestion de plusieurs mots de passe et groupes était plus difficile, notamment lorsqu'il s'agissait de solutions constituées de plusieurs fichiers. Les fichiers peuvent désormais contenir plusieurs tables dans FileMaker Pro 8.5 ; cette nouvelle fonctionnalité semble résoudre les problèmes de gestion du système de sécurité d'un ensemble de fichiers. Il est en effet possible de réduire une solution constituée de plusieurs fichiers en une solution à *fichier unique* de plusieurs tables, dans laquelle toutes les options de sécurité peuvent être gérées de manière centralisée. Si certaines architectures requièrent certes l'approche du *fichier unique* à *plusieurs tables*, il faut cependant reconnaître que dans bien des processus métier et des architectures, des solutions constituées de *plusieurs fichiers* à *plusieurs tables* seront nécessaires. Notons par ailleurs que la conversion d'une solution constituée de plusieurs fichiers FileMaker Pro 6 au format FileMaker Pro 8.5 a pour résultat une solution FileMaker Pro 8.5 constituée de plusieurs fichiers. La gestion d'un schéma de sécurité pour les solutions constituées de *plusieurs fichiers* est donc toujours indispensable.

Les développeurs peuvent désormais accorder aux administrateurs et *superutilisateurs* le droit de gérer des comptes alors que les fichiers sont ouverts et les changements effectués sont appliqués automatiquement. Un *superutilisateur* peut créer un nouveau compte, supprimer, désactiver ou activer un compte existant et réinitialiser le mot de passe d'un compte. Ainsi, le *superutilisateur* a l'autorisation de choisir le mot de passe d'un compte ou peut exiger d'un utilisateur qu'il choisisse un nouveau mot de passe lors de sa prochaine connexion.



Cette permission peut être valable pour tous les fichiers d'une solution. *il n'est pas nécessaire que le superutilisateur ait accès aux schémas de la base de données, comme les tables, les rubriques et les liens pour la gestion des comptes.* Ainsi, les développeurs de solutions commerciales peuvent mettre en place une fonction de gestion de compte assurant la protection de la propriété intellectuelle de leurs solutions.

Le développeur définit les noms et mots de passe de compte à partir du menu *Fichier*, [Fichier-Définir-Comptes et privilèges], le *superutilisateur* quant à lui gère les noms, mots de passe et états de compte via l'utilisation de scripts. Une nouvelle catégorie d'actions de scripts ScriptMaker appelée *Comptes* a été créée à cet effet. Grâce aux options offertes dans l'action ScriptMaker *Ouvrir boîte dial. person.*, l'administrateur ou le *superutilisateur* peut transférer les variables à l'action de script ScriptMaker, par exemple *Créer nouveau compte*. Ceci n'est valable que pour un compte à la fois.

Si le *superutilisateur* souhaite créer cinquante nouveaux comptes *en même temps* dans un ou plusieurs fichiers, les variables adéquates peuvent être transmises de fichier en fichier ; l'action est appliquée graduellement fichier après fichier, compte après compte. Ce processus peut sembler complexe et fastidieux, mais il n'en est rien. Il est possible de créer 1 000 nouveaux comptes dans un seul fichier en moins de deux minutes grâce à cette approche automatisée ; ce processus de script autonome et automatisé transmet les variables requises de Nom de compte et Mot de passe de compte l'une après l'autre d'un fichier de contrôle à un fichier cible.

Outre les actions de script ScriptMaker de gestion de compte, il existe également une nouvelle action ScriptMaker appelée *Reconnexion*, action fort utile en termes de gestion de sécurité. Grâce à cette action, le *superutilisateur* peut se reconnecter à un fichier sous un compte différent sans avoir besoin de fermer le fichier.

Cependant, comment un *superutilisateur* ou un administrateur n'ayant pas accès à un fichier avec un jeu de privilèges [Accès intégral] peut-il contrôler la gestion de la sécurité ? Les développeurs peuvent accorder temporairement à une catégorie d'utilisateurs la possibilité d'exécuter des actions via un script, actions qu'ils ne seraient pas autorisés à effectuer en temps normal. Chaque script est doté d'une option « **Exécuter le script avec tous les privilèges d'accès** » que le développeur peut activer au niveau du script. Le *superutilisateur* peut donc avoir un accès intégral à la gestion de compte via un accès restreint aux scripts de gestion de compte autorisé par un jeu de privilèges subalterne personnalisé, mais avec l'option d'exécution des scripts avec tous les privilèges d'accès activée. La figure 17 illustre l'option « Exécuter le script avec tous les privilèges d'accès » dans la partie inférieure de la fenêtre *Modifier le script*.

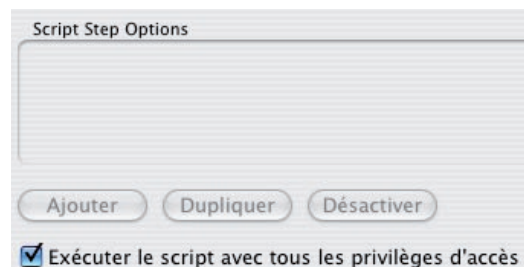


Figure 17. Option d'accès intégral au script.



Lorsque cette option est activée, le script est exécuté¹⁸ comme si l'utilisateur disposait d'un compte doté du jeu de privilèges [Accès intégral] ; notons cependant que les droits sont attribués au *script*, non à l'utilisateur. Associée à la possibilité de rendre un script accessible jeu de privilège par jeu de privilège, cette option permet au développeur d'avoir un contrôle très précis sur les fonctions que chaque utilisateur peut effectuer. A l'aide de cette méthode, un développeur a également la possibilité d'accorder l'accès aux fonctions *Définir la base de données* ou *Définir les références de fichier* à un *superutilisateur* doté d'un compte auquel un jeu de privilèges subalterne personnalisé est affecté. Ce privilège doit bien évidemment être utilisé rarement et avec précaution.

Trafic réseau crypté

Dans les versions antérieures des produits, les logiciels « renifleurs de paquets » pouvaient détecter des paquets de mots de passe FileMaker Pro codés transmis entre réseaux, notamment lorsque les versions antérieures de FileMaker Server les envoyaient codés à un invité pour vérification avant l'accès un fichier.

Dans FileMaker Pro 8.5, l'authentification se produit au niveau du serveur, non du client. Les mots de passe sont quant à eux stockés dans les fichiers¹⁹ ; l'interception est donc beaucoup plus difficile. Enfin, comme mentionné dans la section sur FileMaker Server, le trafic de données réseau est désormais envoyé dans des paquets cryptés. FileMaker Pro 8.5 et FileMaker Server 8 font appel à des algorithmes de sécurité normalisés, éprouvés et reconnus dans tout le secteur.

Les nouvelles versions de FileMaker Pro et de FileMaker Server utilisent la solution de cryptage normalisée TripleDES, couplée à l'algorithme HMAC SHA-1 pour le contrôle de l'intégrité²⁰. TripleDES est un algorithme de cryptage symétrique, créé à partir de son prédécesseur, DES (Data Encryption Standard). L'algorithme DES est une chaîne codée utilisant une clé de 56 bits sur un ensemble de données de 64 bits. Le TripleDES améliore considérablement le DES ; c'est en fait l'algorithme DES appliqué trois fois aux données avec trois clés différentes, soit une clé de 168 bits. L'étude des différents aspects et des fonctions du cryptage symétrique et asymétrique, du cryptage à clé publique, etc. dépasse le propos de cette recommandation technique. Vous trouverez cependant des références dans la bibliographie.

Extraction de mot de passe

L'utilisation de « pirates de mot de passe » a été un véritable défi pour les développeurs FileMaker Pro, cherchant constamment à protéger leur propriété intellectuelle et à assurer l'intégrité et la confidentialité des données des solutions. Ces petits programmes malveillants extraient les mots de passe du fichier et permettent de les ouvrir. Par ailleurs, comme mentionné plus haut, les mots de passe dont le cryptage était simple étaient susceptibles d'être interceptés et décryptés lorsqu'ils transitaient sur un réseau par paquets TCP.

FileMaker Pro 8.5 ne stocke pas les mots de passe dans le fichier de base de données, il stocke une valeur de *hachage* du mot de passe. Celle-ci est le résultat unilatéral et irréversible de l'application d'une règle mathématique sur une chaîne de données. Même si la valeur de hachage²¹ est recouvrée, il est mathématiquement impossible d'en faire l'ingénierie inverse et d'obtenir les données d'origine, en d'autres termes, le *mot de passe*. Lorsque l'utilisateur saisit ses informations d'authentification, FileMaker Pro les crypte et les compare aux valeurs de hachage du fichier. L'utilisateur est validé si les données sont identiques. Les tentatives de piratage des mots de passe n'ont donc que très peu de chance d'aboutir.



Autres problèmes résolus

FileMaker Pro 8.5 s'appuie sur le format de texte Unicode ; les fichiers temporaires sont envoyés aux stations de travail client au format Unicode compressé, ce qui les rend difficiles à lire dans des éditeurs de texte. En outre, le cryptage des fichiers est élevé.

Comme expliqué dans la section sur la *granularité*, FileMaker Pro 8.5 résout le problème rencontré dans les versions antérieures par nombre de développeurs, notamment les développeurs de solutions commerciales, à savoir trouver un équilibre fonctionnel entre la protection de leur propriété intellectuelle d'un côté et de l'autre, des options raisonnables de personnalisation par les utilisateurs finaux. Grâce à la fonction d'attribution de l'autorisation de créer de nouveaux objets, comme des modèles, des scripts et des listes de valeurs sans que les instances existantes de ces objets ne soient affectées, les développeurs disposent d'une bien plus grande flexibilité qu'avant dans la conception de leurs solutions. L'impact sur les modèles métier est également considérable, comme nous le verrons dans la section finale de cette recommandation technique.

Problèmes de conversion depuis des versions antérieures

Nombre de développeurs, de responsables de systèmes informatiques et de gestion de bases de données vont choisir de convertir leurs solutions existantes depuis FileMaker Pro 6 ou des versions antérieures afin de profiter des nombreuses nouvelles fonctions de FileMaker Pro 8.5, FileMaker Server 8 et FileMaker Server 8 Advanced. Selon la structure du schéma de sécurité de ces versions antérieures, des techniques devront être abandonnées, remodelées avant la conversion ou améliorées après la conversion, pour que les fonctions de sécurité offrent les mêmes résultats que précédemment. La conversion est un thème complexe ; il est possible d'y discerner plusieurs nuances ne serait-ce que pour les fonctions de sécurité. Reportez-vous à la documentation supplémentaire disponible sur le site Web FileMaker, Inc. pour de plus amples informations à ce sujet.

La malformation des schémas de sécurité des fichiers FileMaker Pro 6 sera une source essentielle de problèmes au niveau de la conversion. Le manque d'unicité des groupes, le non-respect de la casse des noms de groupes et des mots de passe et l'attribution d'un mot de passe à plusieurs groupes (notamment à des groupes dotés de jeux de privilèges différents) risquent de produire des résultats inattendus dans les fichiers convertis.

Les groupes FileMaker Pro 6 seront convertis en jeux de privilèges FileMaker Pro 8.5 ; le processus tentera de reproduire les anciens privilèges des groupes et les mots de passe associés aussi fidèlement que possible. Cependant, les développeurs doivent vérifier les privilèges convertis ; certains éléments, comme le partage d'un fichier, nécessitent désormais des privilèges étendus pour pouvoir être activés. Si un développeur a créé un groupe dans FileMaker Pro 6 uniquement pour le « mot de passe principal », par exemple un groupe appelé « *Développeur_uniquement* » ou d'une nomenclature similaire, les mots de passe de ce groupe deviendront des comptes liés au jeu de privilèges [Accès intégral] par défaut dans FileMaker Pro 8.5. Dans un effort plus général d'élimination des doublons et de limitation des fichiers mis au rebut, FileMaker Pro 8.5 consolide les groupes dotés de privilèges identiques dans un jeu de privilèges subalterne *unique et unifié*, généralement avec plusieurs noms de compte et mots de passe. Lors de la conversion vers FileMaker Pro 8.5, l'ancien mot de passe FileMaker Pro 6 devient à la fois le nom de compte et le mot de passe du compte. Ainsi, il est facile de connaître les mots de passe, puisque les noms de compte sont visibles lors de leur saisie à la connexion. La première étape pour les développeurs va donc consister à modifier le nom de compte pour qu'il ne soit plus identique au mot de passe.



Par conséquent, des problèmes ne manqueront pas de se produire avec les tests conditionnels s'appuyant sur l'ancien nom de groupe FileMaker Pro 6, comme le prouve la fonction ETAT(GROUPES). La fonction ETAT(GROUPES) est désormais OBTENIR(NOMPRIVILEGES) ; il s'agit là d'une des nouvelles fonctions d'obtention remplaçant les fonctions d'état. Les résultats du test seront différents dans FileMaker Pro 8.5 par rapport à FileMaker Pro 6 si le nom du jeu de privilèges est différent de l'ancien nom de groupe. Ce problème se produit lorsque le jeu de privilèges [Accès intégral] est le résultat d'une conversion depuis un nom de groupe quel qu'il soit vers les « mots de passe principaux » et lorsque des groupes et des mots de passe FileMaker Pro 6 dotés de privilèges identiques mais de mots de passe différents sont consolidés.

Prenons par exemple la syntaxe d'une action de script ScriptMaker basée sur le « mot de passe principal » telle que :

[Si (Occurrences, ETAT(GROUPES), "Développeur_Uniquement")]

La valeur renvoyée dans FileMaker Pro 6 était alors Vrai, mais le test échoue dans FileMaker Pro 8.5 car la syntaxe est désormais [Occurrences (Obtenir(NomPrivilèges), «Développeur_uniquement»)] et le nom du jeu de privilèges est [Accès intégral]. De même, prenons l'exemple de mots de passe dotés de privilèges identiques qui ont été affectés individuellement à des groupes identiques différents, et considérons le test suivant :

[Si (Occurrences, ETAT(GROUPES), "RespsbleVentes")]

La valeur renvoyée dans FileMaker Pro 6 était alors Vrai, mais le test échoue dans FileMaker Pro 8.5 car le groupe « RespsbleVentes » a été consolidé avec des groupes tels que « RespsbleMarketing » et « RespsbleTechnique » dans un jeu de privilèges unique appelé par exemple « RespsbleMarketing ».

Les développeurs doivent vérifier les fichiers convertis afin d'identifier ces anomalies et de les rectifier. Le tableau suivant fournit une liste des emplacements de tels tests, mais n'est pas exhaustive.

Scripts conditionnels [Si...]	Formules de rubrique Calcul
Tests d'Accès aux enregistrements	Valeurs calculées saisies automatiquement
Validation des rubriques par calculs	Listes de valeurs conditionnelles
Actions de script ScriptMaker Définir rubrique et Insérer résultat du calcul	AppleScript ou VB Script généré en partie ou en totalité à partir de rubriques de type Calcul
Fonction Remplace	Fonction Ouvrir boîte de dialogue personnalisée

L'analyse des solutions pour la détection des problèmes éventuels au niveau des schémas de sécurité avant la conversion est essentielle. Nous vous conseillons d'utiliser l'outil DDR de FileMaker Pro 6 Developer ou les outils MetaDataMagic et PasswordAdministrator de New Millennium Communications, Inc. à cette fin²². Portez une attention toute particulière au problème de respect de la casse pour les fichiers d'une même solution. Les mots de passe *Patrick Henry*, *Patrick henry* et *Patrlck henry* sont identiques dans FileMaker Pro 6, mais différents dans FileMaker Pro 8.5²³. Vous pouvez recourir à MetaDataMagic pour identifier les emplacements de ETAT(GROUPES) afin de procéder à une amélioration avant comme après la conversion.



Impact sur les opérations et les modèles métier pour les développeurs et les responsables de systèmes informatiques et de gestion de bases de données

Les nouvelles fonctions de sécurité de FileMaker Pro 8.5 et FileMaker Server 8 auront un profond impact sur le travail des développeurs de solutions commerciales, des développeurs consultants et des responsables de systèmes informatiques et de gestion des bases de données. Par ailleurs, ces nouvelles fonctions affecteront de manière significative les modèles métier sous-tendant les pratiques en matière de conseil de nombre de développeurs.

Depuis plusieurs années, les craintes des développeurs de solutions commerciales en matière de protection de leur propriété intellectuelle n'ont cessé de croître. Dans bien des cas, ces développeurs doivent distribuer leurs solutions dans un format non verrouillé ou en accès intégral afin d'offrir une flexibilité maximale à l'utilisateur final. Parallèlement, ils doivent passer un temps considérable sur la mise à jour des fichiers client, la réimportation de données, la gestion de mots de passe, de groupes et d'autres problèmes d'accès de même nature.

FileMaker Pro 8.5 élimine une grande partie de ce travail supplémentaire. Les développeurs peuvent accorder aux utilisateurs finaux, généralement les administrateurs ou les *superutilisateurs*, le droit de gérer les comptes et de créer toute une série d'objets, notamment des scripts, des modèles et des listes de valeurs *sans* qu'ils aient accès aux instances existantes de ces objets ou que celles-ci soient affectées. En outre, les développeurs commerciaux n'auront plus à craindre que les pirates de mot de passe réussissent à extraire les mots de passe « principaux » de leurs fichiers de solution et utilisent ainsi leurs travaux à des fins non désirées. Enfin, si le développeur de solutions commerciales souhaite intégrer sa solution à une solution client existante, la création de récursions répondant aux appels de la solution client existante et la protection de ces récursions grâce à des privilèges étendus personnalisés ouvrent de nouvelles opportunités en matière de conception et de déploiement de produits.

Les développeurs consultants travaillent eux dans un environnement différent, mettant en place des solutions personnalisées répondant aux besoins spécifiques et aux processus métier d'un client. Le nouveau système de sécurité facilite également ce modèle métier. Les développeurs consultants peuvent se décharger de la responsabilité de gestion des comptes d'utilisateur alors que le personnel de l'entreprise évolue ou voit ses responsabilités et rôles être modifiés. Ils peuvent eux aussi accorder à des *superutilisateurs* la possibilité de créer, d'activer, de désactiver, de supprimer et de réinitialiser des comptes. Ainsi, ils peuvent se concentrer sur l'amélioration des fonctionnalités du système et la création d'éléments de base de données pour répondre aux règles métier client spécifiques, tout au long de la vie d'un projet.

Le personnel informatique peut désormais tirer parti des actifs existants pour gérer la sécurité de toute une gamme d'actifs FileMaker Pro, d'applications de réseaux locaux (LAN) et étendus (WAN), de navigateurs Web et tiers via une connexion ODBC ou JDBC. L'authentification via une connexion unique améliore considérablement les capacités des responsables informatiques à assurer leurs responsabilités en matière de sécurité au niveau global de l'entreprise et simplifie l'ajout ou le retrait d'utilisateurs. L'introduction de flux de données cryptées entre FileMaker Server et les clients FileMaker Pro, dont le moteur de publication Web, aide les responsables informatiques à respecter les normes en matière de sécurité de leur entreprise.



Conclusion

Les nouvelles fonctions de sécurité de FileMaker Pro 8.5, FileMaker Server 8 et FileMaker Server 8 Advanced offrent une approche totalement différente et beaucoup plus efficace de la protection de la propriété intellectuelle, de la confidentialité et de l'intégrité des données. Grâce au contrôle des privilèges sur les objets FileMaker Pro à un niveau granulaire très fin, à l'authentification de compte basée sur les normes du secteur et au cryptage pour la protection des données, le nouveau système de sécurité offre une maîtrise bien plus importante du contrôle de la sécurité qu'autrefois aux développeurs et aux responsables de systèmes informatiques et de gestion de bases de données. Toutes ces fonctions sont disponibles *de facto* dans les fichiers créés avec FileMaker Pro 8.5 ; elles le sont également dès que FileMaker Pro 8.5 convertit un fichier depuis une version précédente.

La sécurité est un thème crucial dont la prise en compte est essentielle ; ce nouveau système offre de nouveaux outils pour assumer cette responsabilité.

A propos de l'auteur

STEVEN H. BLACKWELL est membre Partenaire de l'alliance FSA (FileMaker Solutions Alliance) et président et directeur général de Management Counseling Services [<http://www.FMP-Power.com>]. Lauréat du prix d'excellence FileMaker par deux fois, il est spécialisé dans le développement FileMaker Pro personnalisé, le conseil en sécurité FileMaker Pro et le déploiement FileMaker Server.

Cette recommandation technique est une traduction et adaptation en date du 15 Aout 2006 du document en anglais "Technology Brief - Upgrading to FileMaker 8: How to employ the new, advanced security system" (doc v2).

©2006 FileMaker, Inc. Tous droits réservés. FileMaker est une marque de FileMaker, Inc., déposée aux Etats-Unis et dans d'autres pays. Le logo en forme de dossier et ScriptMaker sont des marques de FileMaker, Inc. Toutes les autres marques sont la propriété de leurs détenteurs respectifs. Les sociétés, organisations, produits, noms de domaine, adresses électroniques, logos, personnes, lieux et événements utilisés en tant qu'exemples sont fictifs. Toute ressemblance avec des personnes ou sociétés existantes serait purement fortuite. Les caractéristiques et la disponibilité des produits sont sujettes à modification sans préavis.

(Doc v2)

LE PRESENT DOCUMENT EST FOURNI « TEL QUEL » SANS GARANTIE DE QUELQUE SORTE, ET FILEMAKER DECLINE TOUTE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS QUE CETTE LISTE SOIT EXHAUSTIVE, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE OU D'ADEQUATION A UN USAGE PARTICULIER, OU LA GARANTIE DE NON-VIOLATION. EN AUCUN CAS, FILEMAKER OU SES FOURNISSEURS NE PEUVENT ETRE TENUS POUR RESPONSABLES DE DOMMAGES QUELS QU'ILS SOIENT (DIRECTS, INDIRECTS, ACCIDENTELS, PERTE DE BENEFICES D'EXPLOITATION, DOMMAGES PUNITIFS OU SPECIAUX), MEME SI FILEMAKER OU SES FOURNISSEURS ONT ETE INFORMES DE L'EVENTUALITE DE CES DOMMAGES. CERTAINS ETATS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DE RESPONSABILITES. FILEMAKER PEUT APPORTER DES MODIFICATIONS AU PRESENT DOCUMENT A TOUT MOMENT, SANS PREAVIS. LE PRESENT DOCUMENT N'EST PEUT-ETRE PAS A JOUR, ET FILEMAKER NE S'ENGAGE PAS A METTRE A JOUR CES INFORMATIONS.



(Notes de fin de document)

¹ Bruce Schneier, fondateur de Counterpane Labs, première entreprise de sécurité numérique, a longuement évoqué ces questions avec éloquence et pertinence dans son livre *Secrets & Lies Digital Security in a Networked World*, New York, NY. John Wiley & Sons. 2000. Traduit en français : *Secrets et mensonges. Sécurité numérique dans un monde en réseau*.

² Voir l'article numéro 967 de base de connaissances TechInfo FileMaker, Inc., ainsi que le livre blanc *Web Security* disponible sur le site Web FileMaker, Inc. pour de plus amples informations à ce sujet.

³ Un groupe de domaine de type Active Directory ou Open Directory, non un ancien groupe FileMaker Pro 6.

⁴ Vous pouvez rencontrer des problèmes si vous utilisez certains caractères non alphanumériques ASCII supérieurs pour accéder à des comptes Web dans FileMaker Pro 8.5. Reportez-vous au *Guide de la publication Web* au format PDF sur le site Web FileMaker, Inc. pour de plus amples informations.

⁵ Dans le menu *Fichier*, sélectionnez Options de fichier...-Ouvrir/Fermer et désactivez la connexion automatique.

⁶ Comme défini par Active Directory ou Open Directory.

⁷ Compte dont le jeu de privilèges attribue un accès complet et non limité à toutes les parties du fichier. Cette notion correspond plus ou moins au concept de « mot de passe principal » de FileMaker Pro 6. Cependant, ce terme n'est plus valable et n'est pas utilisé dans FileMaker Pro 8.5.

⁸ Il existe nombre de ressources à ce sujet, une sélection est disponible dans la bibliographie de cette recommandation technique.

⁹ Le nom de compte et le mot de passe peuvent être identiques au jeu de privilèges, par exemple *Responsible Marketing* ou *Ventes*. Assurez-vous simplement de supprimer ces comptes tests une fois le processus de développement terminé. Les nouveaux comptes valides peuvent ensuite être affectés à chaque jeu de privilèges.

¹⁰ Voir le numéro de janvier 2004 du magazine *FileMaker Advisor* pour de plus amples informations sur l'accès à partir des rôles.

¹¹ Cette fonction renvoie le nom du compte ayant accès au fichier. Dans le cas d'une authentification externe, elle renvoie également le nom du compte et non le nom du groupe. Voir la discussion sur l'ordre d'authentification.

¹² Les bases de données converties configurées sur la saisie automatique du Nom du créateur ou du Nom du modificateur dans les versions antérieures peuvent être définies sur le Nom de compte dans les options de saisie automatique des définitions de rubriques. Dans ce cas cependant, le fichier converti doit être ajusté de sorte que les noms de compte soient similaires aux noms d'utilisateur et *vice versa*, notamment si les tests d'accès aux enregistrements dépendent de ces données.

¹³ Le véritable problème de sécurité ici est le suivant : en autorisant leur création, le développeur autorise également la modification des objets de la même classe qu'il a créés.



¹⁴ Voir la recommandation technique FileMaker, Inc. sur FileMaker Server 8 rédigé par Wim Decorte pour de plus amples informations sur la connexion.

¹⁵ Un groupe de domaine de type Active Directory ou Open Directory, non un ancien groupe FileMaker Pro 6.

¹⁶ Vous pouvez notamment placer le moteur de publication Web (WPE) et IIS/Apache sur la même UC en utilisant un réseau VPN s'ils se trouvent sur deux UC différentes comme c'est probablement le cas, ou encore créer un réseau fermé entre l'UC de FileMaker Server 8, celle du WPE et celle d'Apache/IIS. La mise en place de ces types de configuration est facilitée par les capacités de rattachement multiple offertes par FileMaker Server 8. Voir les recommandations techniques sur FileMaker Server et la publication Web FileMaker. La logique voudrait que le WPE et IIS/Apache soient exécutés sur la même UC et que des pare-feu soient activés pour garantir la confidentialité des données. Toutefois, les UC équipées de deux processeurs sont particulièrement adaptées pour ce type de configuration.

¹⁷ Voir la recommandation technique FileMaker, Inc. sur la publication Web FileMaker 8 rédigé par Cris Ippolite pour de plus amples informations.

¹⁸ Cette option doit également être activée pour chaque sous-script appelé, si celui-ci doit effectuer une action nécessitant les privilèges [Accès intégral].

¹⁹ Cela signifie également qu'ils ne sont pas visibles sur l'interface utilisateur : ils sont cachés lors de leur saisie et le restent tout le temps.

²⁰ Voir la page <http://java.sun.com/j2se/1.4.2/docs/guide/security/jce/JCERefGuide.html> pour une description approfondie du code d'authentification de message haché (HMAC, Hashed Message Authentication Code en anglais).

²¹ Voir la page <http://searchtechtarget.techtarget.com> pour de plus amples informations sur les valeurs de hachage.

²² <http://www.newmillennium.com>

²³ N'oubliez pas que les utilisateurs devront respecter la casse dans le choix de leurs mots de passe.

Bibliographie

Ouvrages

Alberts, Christopher J. et Dorofee, Audrey J. *Managing Security Risks The OCTAVE™ Approach* (Addison-Wesley, New York, NY, 2002)

Barrett, Diane; Hausman, Kirk et Weiss, Martin. *Security+* (Que, Indianapolis, IN, 2003)

Schneier, Bruce. *Secrets & Lies Digital Security in a Networked World* (John Wiley & Sons, New York, NY, 2000).

Singh, Simon. *The Code Book* (Anchor Books, New York, 1999)



Strebe, Matthew *Network Security Jumpstart* (Sybex, San Francisco, 2002)

Articles

“Internet Security” *Time*, 7/2/2001

Andress, Mandy, and Edward, Mark T. “Beware Wireless Security Woes” *E Business Advisor* March 2002

Chang, Stephanie and Janowski, Davis D. “The lay of the wireless LAN” *PC Magazine*, 5/21/2002

Hawkins, Dana. “Hide and they can’t seek” *US News & World Report* 5/19/2003

Kerstetter Jim and Weintraub, Arlene. “Cyber Alert Portrait of an Ex-Hacker” *Business Week*, 6/9/2003

Kerstetter Jim. “You’re Only As Good As Your Password” *Business Week*, 9/2/2002

Marelia, Darren. “AD network Interactions” *Windows & .Net magazine*, 3/1/2003

Vacca, John R. “Save Money With a Secure Remote-Access VPN” *Business Security Advisor*, July/August 2002

