

## LA SECURITE ACCES POUR VISIONIC

Afin de répondre aux exigences de sécurité définies lors du dernier Comité de Pilotage VISIODENT qui s'est tenu à Evry le 10 mars dernier, la version 4.0 de VISIONIC dispose désormais d'outils permettant de définir les droits des divers utilisateurs du logiciel.

La mise en place de la **sécurité au niveau utilisateurs** (c'est le terme consacré), permet de créer des groupes d'utilisateurs disposant d'autorisations à effectuer telle ou telle action.

En **annexe II** vous trouverez un document (récupéré sur Internet) qui traite en détail de tous les aspects de la sécurité sous ACCESS et qui vient étayer mon propos.

Cette sécurisation s'accompagne de contraintes lourdes qu'il faut bien comprendre pour pouvoir mettre en œuvre efficacement le logiciel. C'est malgré tout le seul gage d'une sécurité optimale.

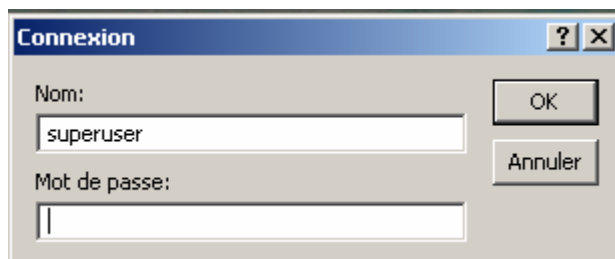
Tout d'abord la sécurité sous ACCESS est subordonnée à la création d'un *espace de travail* qui accueille les divers groupes d'utilisateurs. Il est important de définir un espace de travail particulier à VISIONIC afin de ne pas perturber les autres bases de données ACCESS déjà en service sur les postes de travail.

C'est également un élément de sécurité important, car les bases VISIONIC.mdb et VISIODATA.mdb ne pourront plus être ouvertes par un utilisateur lambda hors du contexte de sécurité défini par l'*espace de travail*.

Cet *espace de travail* est stocké dans un fichier .mdw, en l'occurrence VDTOCOP.mdw, que nous placerons dans le répertoire C:\VISIONIC avec VISIODATA.mdb dans un souci de simplification.

Pour pouvoir lancer VISIONIC dans le bon contexte, il faudra impérativement créer des raccourcis sur le bureau, car le lancement d'ACCESS nécessite un paramétrage. L'option /wrgrp suivie du chemin de stockage du fichier mdw suivie éventuellement d'une option /user avec le nom de l'utilisateur qui va se servir de VISIONIC. Cette dernière option est pratique si l'on ne gère pas de mot de passe pour les utilisateurs de base (qui je le rappelle ne disposeront que de droits limités) car elle évite de passer par la phase d'authentification.

Un raccourci sera également nécessaire pour l'administrateur, qui disposera obligatoirement d'un mot de passe et qui passera donc par la phase d'authentification dont voici la fenêtre :



Un point important de la sécurité sous ACCESS réside dans la possibilité offerte aux utilisateurs de voir les objets de la base (Tables, Requêtes, Formulaires, Etats, Macros, Modules). Même dans un contexte fermé avec des options de démarrage sensées masquer certaines choses, MICROSOFT a prévu une porte de service connue de beaucoup d'utilisateurs (je ne dirai pas laquelle pour laisser le plaisir de la recherche à ceux qui ne la connaissent pas).

Il faut donc également verrouiller cette porte pour avoir la certitude que les utilisateurs non autorisés ne puissent pas modifier le contenu d'un enregistrement en dehors des processus définis par programmation.

Il faut néanmoins permettre les opérations de maintenance aux utilisateurs avertis, qui doivent disposer de la clé du verrou. Une image de cadenas (ouvert ou fermé) a été rajoutée à la page d'accueil de VISIONIC permettant de vérifier que le verrou est bien fermé. Si c'est le cas **même l'administrateur** de la base n'aura pas accès aux données en lecture directe. Par contre il aura accès au verrou.

## GESTION DES GROUPES ET DES UTILISATEURS

Comme il a été dit plus haut, un *espace de travail* se compose d'utilisateurs pouvant appartenir à des groupes spécifiques (créé par la cause) ou aux groupes par défaut qui sont au nombre de deux.

Le groupe Administrateurs qui comme son nom l'indique regroupe tous les administrateurs qui disposent de droits étendus et du privilège d'attribuer ou d'enlever les droits aux autres utilisateurs.

Le groupe Utilisateurs dont les membres disposent des seuls droits qui leur sont attribués.

L'administrateur par défaut (fourni par Microsoft) a été annihilé (c'est un principe de précaution, car il ne peut pas être supprimé). Il ne sert donc plus à rien.

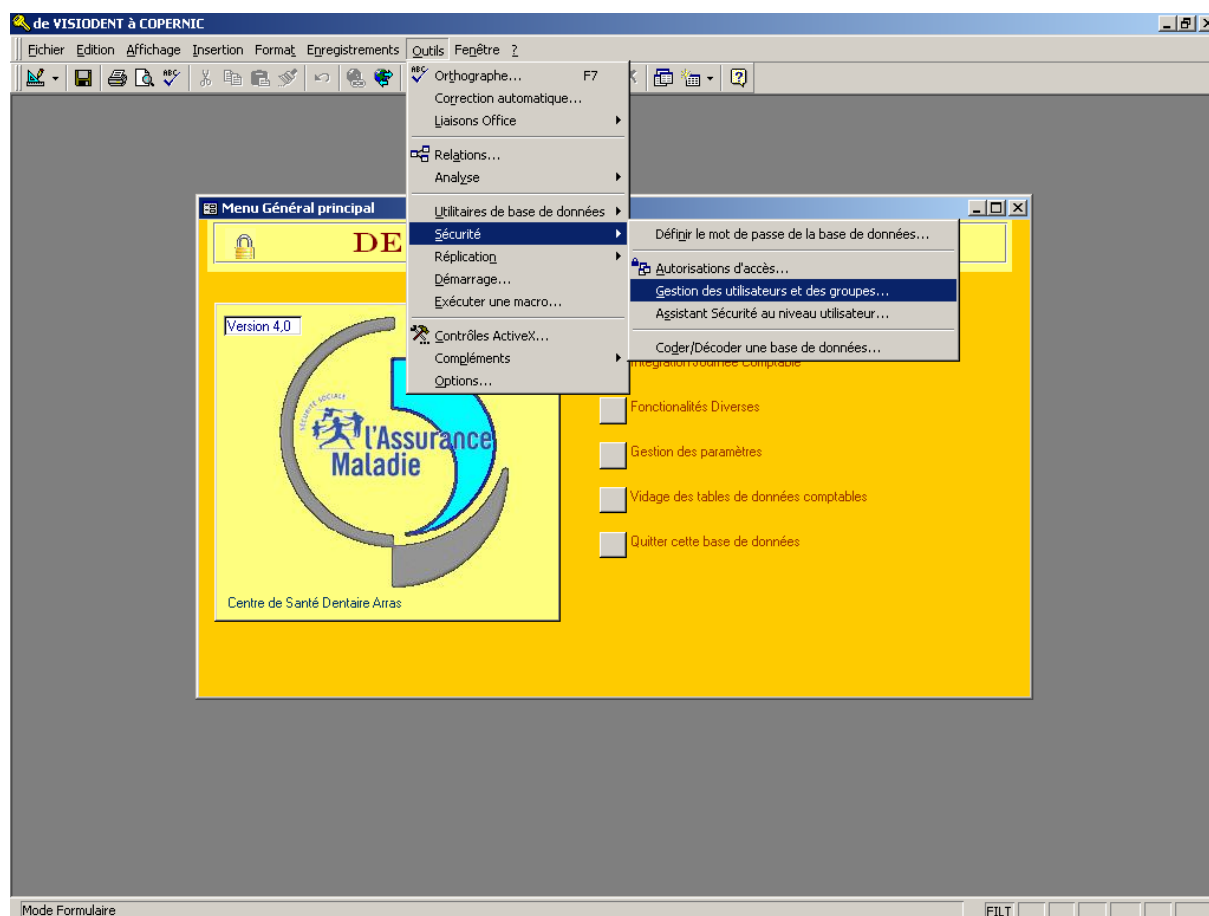
J'ai créé un nouvel administrateur qui s'appelle **superuser** et dont le mot de passe est **ESCALIBUR** en majuscule.

Cet administrateur appartient au groupe Administrateurs (ce qui semble normal), mais également au groupe Utilisateurs (ce qui ne sert à rien) mais cela est incontournable.

Le groupe Administrateurs doit avoir tous les droits sur tous les objets des deux bases (VISIONIC et VISIODATA) pour pouvoir permettre au superuser de faire correctement son travail.

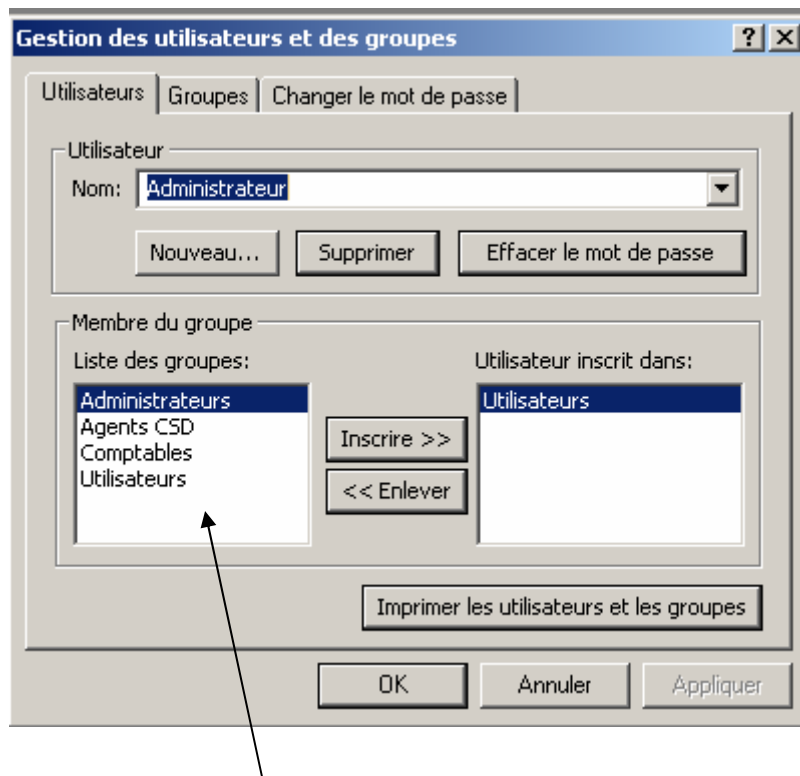
La notion de groupe, vous l'avez compris, permet de gérer les autorisations au sens large. Il est alors possible de créer autant d'utilisateurs que l'on veut et de rattacher ces derniers à un groupe pour qu'ils héritent automatiquement des droits du groupe. Même s'il est possible de donner des droits spécifiques au niveau utilisateur, il apparaît plus commode de se cantonner au niveau des groupes pour gérer les droits.

Voici comment les choses se présentent :



**Attention, pour pouvoir accéder à ce qui suit, il faut être le superuser, et avoir déverrouillé la base. Il faut ensuite sortir de VISIONIC et accéder de nouveau à VISIONIC par la porte de service. Pensez à bien verrouiller à nouveau la base avant de quitter VISIONIC sinon tout ce qui suit ne sert à rien.**

Dans VISIONIC (les groupes et utilisateurs seront les mêmes pour VISIODATA) cliquez sur le menu *Outils*, puis *Sécurité*, puis *Gestion des Utilisateurs et des Groupes*, vous obtiendrez la fenêtre suivante :



J'ai créé un groupe *Agents CSD* et un groupe *Comptables*.

J'ai défini des autorisations limitées pour chacun de ces deux groupes.

Compte tenu que les utilisateurs de base doivent disposer de droits assez étendus sur les données (hormis les paramètres) et que de plus vous n'êtes pas sensés connaître tous les droits dont ils doivent disposer pour mener à bien telle ou telle action, ils disposent de tous les droits sur les objets de type tables requêtes, états, macros et modules. Ceci n'est pas gênant puisqu'ils ne peuvent plus accéder à ces objets autrement que par programmation.

Il vous faut donc, si le modèle de base ne vous convient pas, limiter votre action aux seuls formulaires qui sont ouverts depuis le menu général de l'application. Ainsi si vous ne voulez pas que tel groupe puisse modifier les paramètres vous interdisez la lecture de chaque formulaire de gestion des paramètres.

Voici l'écran qui vous permettra de mieux comprendre. Il est accessible, en cliquant sur *Outils*, puis *Sécurité* et enfin *Autorisations d'accès*

Vérifiez que vous êtes bien sur Groupes

Attention au type d'objet

Dans l'exemple ci-dessus, le groupe Agents CSD dispose de l'autorisation d'exécuter le formulaire Cfactures, qui permet de consulter une facture dans VISIONIC. En **Annexe I** vous trouverez la liste de tous les formulaires, de leur fonction, et des autorisations actuellement disponible.

Dans VISIODATA, il n'y a que des objets de type table. Il est possible de mettre des restrictions d'accès sur les tables de paramètres qui sont en lecture seule dans l'application (identification de la structure, gestions, comptes avec et sans mode, débiteurs). En fait seule la table Cliniques ne peut pas être protégées au niveau table, mais seulement au niveau formulaire. Ceci vous permettra donc d'autoriser (sauf pour la table Cliniques) la consultation des paramètres par les utilisateurs de bases, mais pas la modification, l'ajout et la suppression.

Sur le modèle de sécurité fourni, seule le superuser a des droits sur ces tables. Les groupes Agents CSD et Comptables ne peuvent que les consulter.

En clair, je vous fournis une sécurité avec trois Groupes trois utilisateurs de base et trois niveaux de protection.

Le groupe Administrateurs avec l'utilisateur superuser disposant d'un accès total à VISIONIC et VISODATA, pour le paramétrage et la maintenance des bases. Il peut faire fonctionner l'application mais ce n'est pas son rôle, il n'est donc pas souhaitable de s'en servir pour ça.

Le groupe Comptables avec l'utilisateur comptable disposant d'un accès total à toutes les fonctions de l'application, sauf la restauration d'une sauvegarde, la sécurisation de la base, et le vidage des tables comptables. Il peut visualiser les paramètres (sauf cliniques) mais pas les modifier.

Le groupe Agents CSD avec l'utilisateur caissière disposant des mêmes droits que le comptable sauf sur la visualisation des paramètres.

Ceci reste évidemment un modèle qui peut-être modifié à votre convenance.

## ANNEXE I – DEFINITION DES FONCTIONS SECURISEES FOURNIES PAR DEFAULT

FORMULAIRE	ACTION	Autorisations Des Groupes*		
		Administrateurs	Comptables	Agents CSD
Cfactures	Fonctionnalités Diverses\Visualisation Factures	TOTALE	EXEC	EXEC
Cliniques	Gestion des paramètres\Cliniques	TOTALE	AUCUNE	AUCUNE
Comptes Avec Mode	Gestion des paramètres\Comptes Avec Mode	TOTALE	CONSULT	AUCUNE
Comptes Sans Mode	Gestion des paramètres\Comptes Sans Mode	TOTALE	CONSULT	AUCUNE
Controles	Sous formulaire\Inégration	TOTALE	EXEC	EXEC
Debiteurs	Gestion des paramètres\Débiteurs	TOTALE	CONSULT	AUCUNE
Détail Règl. Assurés	Sous formulaire\Cfactures	TOTALE	EXEC	EXEC
Détail Règlements RC	Sous formulaire\Cfactures	TOTALE	EXEC	EXEC
Détail Règlements RO	Sous formulaire\Cfactures	TOTALE	EXEC	EXEC
Gestion	Gestion des paramètres\Gestions	TOTALE	CONSULT	AUCUNE
IdentStruc	Gestion des paramètres\Identification Structure	TOTALE	CONSULT	AUCUNE
Importation	Importation des données de VISIODENT	TOTALE	EXEC	EXEC
Integration	Intégration Journée Comptable	TOTALE	EXEC	EXEC
ListDtx	Fonctionnalités Diverses\Régl. Clients Douteux	TOTALE	EXEC	EXEC
Menu Général	Sans commentaire	TOTALE	EXEC	EXEC
RazDats	Vidage des tables de données comptables	TOTALE	ANCUNE	AUCUNE
RcptRembC	Sous formulaire\Remboursements	TOTALE	EXEC	EXEC
RcptRembD	Sous formulaire\Remboursements	TOTALE	EXEC	EXEC
RcptVentC	Sous formulaire\Ventilation	TOTALE	EXEC	EXEC
RcptVentD	Sous formulaire\Ventilation	TOTALE	EXEC	EXEC
RegDtx	Sous formulaire\ListDtx	TOTALE	EXEC	EXEC
Remboursements	Sous formulaire\Controles	TOTALE	EXEC	EXEC
Restauration	Fonction. Diverses\Restauration des données	TOTALE	AUCUNE	AUCUNE
Sauvegarde	Fonction. Diverses\Sauvegarde des données	TOTALE	EXEC	EXEC
Sécur	Fonctionnalités Diverses\Sécurisation de la base	TOTALE	AUCUNE	AUCUNE
Soldes	Fonctionnalités Diverses\Etat des Soldes	TOTALE	EXEC	EXEC
TotSoldes	Sous formulaire\Soldes	TOTALE	EXEC	EXEC
ValidJoc	Sous formulaire\Intégration	TOTALE	EXEC	EXEC
Ventilation	Sous formulaire\Controles	TOTALE	EXEC	EXEC

(\*) explication sur les autorisations : TOTALE signifie toutes les autorisations – indispensable pour les administrateurs. EXEC signifie que le groupe peut ouvrir le formulaire et exécuté le code sous-jacent. CONSULT signifie que compte tenu des restrictions évoquées plus haut sur les tables de paramètres contenues dans VISIODATA, par défaut le groupe Comptables ne dispose que de la visualisation sur des tables. AUCUNE implique que le groupe ne peut pas ouvrir, ni exécuter le code du formulaire. ACCESS renvoie un message qui n'est pas très causant mais l'action est bloquée ce qui est le principal.

# **LA SECURITE SOUS ACCESS '97**

# La sécurité dans MS ACCESS

## Protection d'une base de données

Microsoft Access offre trois méthodes de protection d'une base de données :

- définir un **mot de passe** pour ouvrir une base de données
- enregistrer la base de données dans un **fichier au format MDE**, ce qui supprime le code Visual Basic modifiable et empêche la modification de la structure des formulaires, des états et des modules.
- utiliser une **sécurité au niveau utilisateur**, ce qui permet de délimiter les parties auxquelles l'utilisateur peut accéder ou celles qu'il peut modifier.

## Définition d'un mot de passe

La méthode la plus simple est de définir un mot de passe pour ouvrir la base de données. Dès qu'un mot de passe est défini, une boîte de dialogue qui exige un mot de passe s'affiche lors de chaque ouverture de la base de données. Seul les utilisateurs qui tapent le mot de passe correct pourront ouvrir la base de données.

Cette méthode est sûre (Microsoft Access code le mot de passe pour qu'il ne soit pas accessible en lisant directement le fichier de base de données), mais elle ne s'applique qu'à l'ouverture d'une base de données. Dès qu'une base de données est ouverte, tous ses objets sont à la disposition de l'utilisateur. Pour une base de données qui est partagée entre un petit groupe d'utilisateurs, ou sur un ordinateur isolé, définir un mot de passe est souvent suffisant.

Marche à suivre :

- 1° Fermer la base de données. Si la base de données est partagée sur un réseau, demander aux autres utilisateurs de fermer la base de données.
- 2° Faire une copie de sauvegarde de la base de données et la stocker dans un endroit où elle sera en sécurité !
- 3° Dans le menu Fichier de ACCESS, cliquer sur Ouvrir une base de données.
- 4° Activer la case à cocher « Mode exclusif », avant d'ouvrir la base de données.
- 5° Menu « Outils » - « Sécurité » - « Définir le mot de passe de base de données ».
- 6° Dans la zone Mot de passe, taper le mot de passe et le confirmer.
- 7° Valider.

Le mot de passe est à présent défini. La prochaine fois que tout utilisateur ouvrira la base de données, une boîte de dialogue demandant le mot de passe s'affichera.

Attention :

- Un mot de passe respecte la casse; on doit le taper exactement comme il a été défini.
- Si on perd ou si on oublie le mot de passe, il ne peut pas être récupéré et plus personne ne pourra pas ouvrir la base de données !

## Enregistrement d'une base de données dans un fichier MDE

Si la base de données comporte du code Visual Basic, en l'enregistrant comme fichier MDE on permet de compiler tous les modules, de supprimer tout le code source modifiable et de compacter la base de données de destination. Le code Visual Basic sera toujours exécuté, mais il ne pourra plus être visualisé ni modifié ; de plus, la base de données prendra moins de place car le code est supprimé et l'utilisation de la mémoire est optimisée, ce qui augmente les performances.

L'enregistrement de la base de données comme fichier MDE, empêche les opérations suivantes :

- Afficher, modifier ou créer des formulaires, des états ou des modules en mode Création.
- Ajouter, supprimer ou modifier des références aux bases de données.
- Modifier le code Visual Basic, car le fichier MDE ne contient aucun code source.
- Changer le nom du projet VBA de la base de données à l'aide de la boîte de dialogue Options.
- Importer ou exporter des formulaires, des états ou des modules. Par contre, il est toujours possible d'importer ou d'exporter des tables, des requêtes ou des macros à partir ou vers des bases de données non MDE.

Attention :

Il faut absolument effectuer une **copie** de la base de données d'origine. Si l'on désire modifier ultérieurement la structure d'un formulaire, d'un état ou d'un module d'une base de données enregistrée au format MDE, on doit effectuer ces modifications **dans la base de données d'origine**, puis l'enregistrer à nouveau comme fichier MDE.

C'est pour cette raison qu'il faut éviter d'enregistrer comme fichier MDE une base de données comportant des **tables**... On ne pourra pas simplement modifier la structure d'un formulaire, d'un état ou d'un module dans la version d'origine, car les données des tables qu'elle contient ne sont plus à jour ! Il est plutôt conseillé de choisir la base de données frontale qui contient toute la structure de gestion (requêtes, formules, états, modules) pour l'enregistrer comme fichier MDE, alors que la base qui contient les tables se contentera d'être liée.

Marche à suivre :

- 1° Fermer la base de données. Dans un environnement multi-utilisateur, tous les utilisateurs doivent fermer la base de données.
- 2° Menu « Outils » - « Utilitaires de base de données » - « Créer fichier MDE. ».
- 3° Dans la boîte de dialogue « Base de données à enregistrer comme MDE », indiquer la base de données que l'on désire enregistrer comme fichier MDE et cliquer sur « Créer MDE ».
- 4° Dans la boîte de dialogue « Enregistrer MDE comme », indiquer le **nom**, l'**unité** et le **dossier** de la base de données.

## Sécurité au niveau utilisateur

La méthode la plus flexible et la plus étendue pour protéger une base de données s'appelle la sécurité au niveau utilisateur. Ce type de sécurité est similaire aux méthodes utilisées dans la plupart des systèmes de réseau. Les utilisateurs doivent s'identifier et taper un mot de passe lorsqu'ils démarrent Microsoft Access. Au sein du fichier d'informations de groupe de travail, ils sont identifiés comme étant les membres d'un groupe. Microsoft Access fournit deux groupes par défaut : les administrateurs (appelés le groupe Administrateurs) et les utilisateurs (appelés le groupe Utilisateurs), mais des groupes supplémentaires peuvent être définis.

Les autorisations d'accès sont accordées aux groupes et aux utilisateurs pour déterminer de quelle manière ils sont autorisés à travailler avec chaque objet dans une base de données. Par exemple, les membres du groupe Utilisateurs pourraient être autorisés à visualiser, introduire ou modifier des données dans une table Clients, mais ils ne pourraient pas changer la présentation de cette table. Le groupe Utilisateurs pourrait être autorisé à visionner les données de certaines tables et se voir refuser l'accès total à une table Salaires. Les membres du groupe Administrateurs ont toutes les autorisations d'accès sur tous les objets d'une base de données.

Les trois raisons principales d'utilisation de la sécurité au niveau utilisateur sont :

- Protéger la propriété intellectuelle du code.
- Éviter que les utilisateurs ne détériorent par inadvertance une application en changeant le code ou les objets dont l'application dépend.
- Protéger des données essentielles dans la base de données.



Les groupes, les utilisateurs, les bases de données et toutes les autorisations d'accès font partie d'un **environnement commun** qu'on appelle un **espace de travail** (Work Space).

### Espace de travail et fichier System.mdw

Dans ACCESS, le système de sécurité est **toujours en activité** :

- on appartient toujours à un espace de travail
- on fait toujours partie d'un groupe
- on est toujours un utilisateur !

Ces diverses informations sont stockées dans un fichier discret, mais très important, que l'on trouve au premier niveau de l'environnement d'installation d'ACCESS, soit dans MSOFFICE ou dans ACCESS lui-même pour les machines en réseau, soit dans Windows\System pour les machines autonomes : le fichier **system.mdw**.

Nom	Dans le dossier	Taille	Type
system.mdw	H:\MSOffice	72 Ko	Informations sur le groupe de travail Microsoft Access
Msaccess.exe	H:\MSOffice\office	2'929...	Application

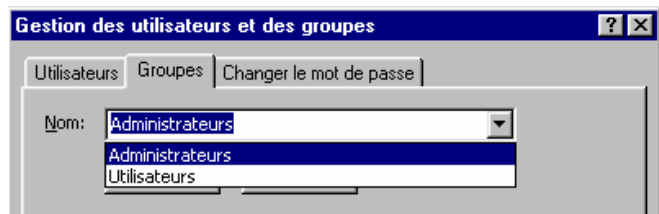
MDW = Microsoft Data Workspace

C'est le « **fichier d'informations du groupe de travail** » comme l'appelle Microsoft. Ce fichier est créé au moment de l'installation du logiciel sur la machine. Les paramètres nécessaires à la génération de ce fichier sont pris dans les deux informations que l'on doit fournir lors de l'installation : le nom de l'utilisateur de la machine et le nom de l'organisation dans laquelle il travaille.

Par défaut, tout personne qui lance ACCESS va se trouver englobée dans l'**espace de travail** défini par ce fichier « System.mdw » :

1° Cet espace contient deux groupes :

- les Administrateurs Admins
- les Utilisateurs Users



2° Cet espace abrite deux utilisateurs :

- Un Administrateur Admin
- Un Utilisateur standard Guest



Remarques :

- Dans la version française, les termes anglais ont été traduits, mais il faut utiliser les termes anglais en Visual Basic.
- Il arrive que l'utilisateur standard (Guest) ne soit pas créé dans l'espace de travail. On n'aura donc que l'Administrateur (Admin) à disposition...
- Le(s) utilisateur(s) mentionné(s) n'ont pas de mot de passe !

**Les dangers de l'espace de travail « par défaut »**

**Principe :** Quand on lance ACCESS sans indication particulière,

- on utilise toujours l'espace de travail par défaut décrit pas System.mdw
- on est toujours considéré comme l'Administrateur de cet espace de travail.

**Conséquence :** En tant qu'**Administrateur**, on a **tous les pouvoirs** sur l'espace de travail en cours, ainsi que sur toutes les bases de données créées à partir de cet espace et, bien entendu, sur tous les objets que peuvent contenir ces bases !

### Risque :

Le premier utilisateur un peu futé et mal intentionné attribue un mot de passe à l'Administrateur ...

Il devient le propriétaire de l'espace de travail et, à partir de cet instant, il empêche tous les autres utilisateurs ... d'utiliser toutes les bases de données déjà créées à partir de cet espace de travail !

The screenshot shows a Windows-style dialog box titled "Gestion des utilisateurs et des groupes". It has three tabs: "Utilisateurs", "Groupes", and "Changer le mot de passe". The "Changer le mot de passe" tab is selected. Inside the dialog, there are four labels with corresponding input fields: "Nom de l'utilisateur:" with the text "Administrateur", "Ancien mot de passe:", "Nouveau mot de passe:", and "Confirmation:". The input fields for the password are empty.

### Précautions à prendre :

- Interdire la modification du fichier System.mdw à tous les utilisateurs (répertoire protégé).
- Garder une copie du fichier System.mdw en lieu sûr pour remplacer la version qui serait modifiée par un utilisateur malveillant.
- Organiser et administrer un ou plusieurs espaces de travail bien protégés.

### Création d'un nouvel espace de travail

Il faut exécuter le programme WRKGADM.EXE (WoRK Group ADMinistrator) qui se trouve, soit dans Windows\System, soit dans l'environnement Access, pour pouvoir créer un nouveau fichier System.mdw.

Comme on le voit, ce fichier n'est pas tiré du néant, mais est « copié » à partir d'un fichier existant : cela peut être l'original ou déjà une version préparée par nos soins.

The screenshot shows a dialog box titled "Administrateur de groupe de travail". It contains three labels with text: "Nom:" with the value "Charles Eberhard", "Organisation:" with the value "Personnel", and "Fichier de groupe de travail:" with the value "C:\WINDOWS\SYSTEM\system.mdw". Below these fields is a paragraph of text: "Le groupe de travail est défini par le fichier d'informations utilisé au démarrage. Il est possible de créer un nouveau groupe en créant un nouveau fichier d'informations, ou de joindre un groupe existant en changeant le fichier d'informations du démarrage." At the bottom, there are three buttons: "Créer...", "Joindre...", and "Quitter".

**Note :** La dénomination «groupe de travail» n'est pas très heureuse : il vaudrait mieux parler d'un « espace de travail », terme utilisé dans Visual Basic. Le mot groupe peut prêter à confusion, car on va définir des groupes d'utilisateurs à l'intérieur du « groupe de travail »...

Trois informations sont nécessaires pour générer le nouveau fichier :

- Le nom
- L'organisation
- Le Code groupe de travail.

Le « code groupe de travail » doit assurer que l'espace de travail que l'on crée est réellement **unique**, car la même personne (Nom), dans la même entreprise (Organisation), peut créer plusieurs « groupes de travail ». Ce code est donc le seul moyen de les distinguer !

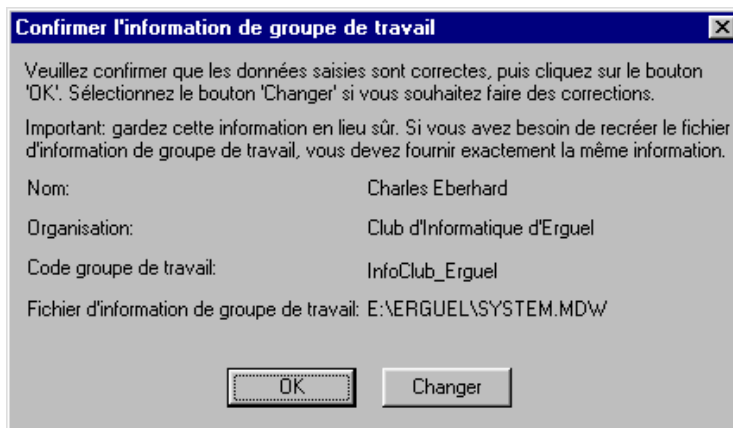
The screenshot shows a form with three input fields. The first field is labeled "Nom:" and contains the text "Charles Eberhard". The second field is labeled "Organisation:" and contains the text "Club d'Informatique d'Erguel". The third field is labeled "Code groupe de travail:" and contains the text "InfoClub\_Erguel".

On peut donner un nouveau nom au fichier créé et le stocker dans le même répertoire que le fichier « System.mdw » d'origine, ou enregistrer le nouveau « System.mdw » dans un répertoire particulier qui sera partagé par les différents utilisateurs de ce « groupe de travail ».

Il est vital de conserver les paramètres utilisés, par écrit et dans un endroit sûr.

En effet, si le fichier « d'informations du groupe de travail » venait à être détruit ou corrompu, la seule façon de pouvoir accéder aux bases de données partageant cet espace de travail est de reconstruire un fichier identique !

Attention : Il faut absolument respecter les majuscules et les minuscules d'origine. Les Américains parlent de « case sensitive » !



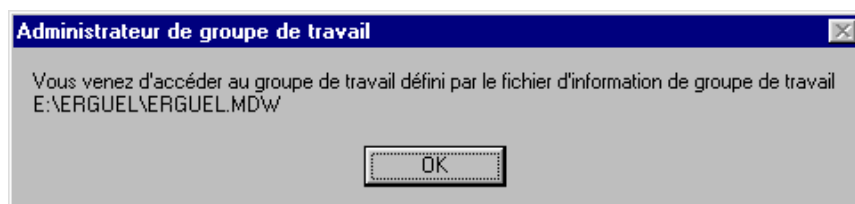
### Choix d'un espace de travail particulier

Nous avons maintenant plusieurs espaces (groupes) de travail. Comment faire pour indiquer celui avec lequel on veut travailler ? Dans sa version française, Microsoft parle de « rejoindre un groupe de travail Microsoft Access ».

Deux méthodes sont possibles :

#### 1° Utiliser le programme « Administrateur de groupe de travail »

- Démarrer Wrkgadm.exe (l'Administrateur de groupe de travail) qui doit se trouver dans le sous-dossier Système du dossier Windows.
- Dans la boîte de dialogue, cliquer sur « Joindre ».
- Taper le chemin d'accès et le nom du fichier d'informations de groupe de travail qui définit le groupe de travail Microsoft Access que l'on veut rejoindre ou utiliser « Parcourir » pour localiser et sélectionner le fichier d'informations du groupe de travail désiré.



Ce chemin a été sauvegardé dans la base de registres sous la clé :

Hkey\_Local\_Machine\Software\Microsoft\Office\8.0\Access\Jet\3.5\Engines

Au démarrage suivant, Microsoft Access utilisera automatiquement les informations stockées dans le fichier .MDW du groupe de travail que l'on vient de « rejoindre ».

#### 2° Démarrer ACCESS avec une option sur la ligne de commande

Il suffit d'ajouter l'option **/wrkgrp** à la ligne de commande.

Exemple : F:\MsOffice\Office\Msaccess.exe /wrkgrp E:\Erguel\Erguel.mdw

On peut taper cette ligne dans la fenêtre « Démarrer » - « Exécuter » ou prévoir un raccourci sur le bureau ou dans le menu « Démarrer ».

Attention : Avec des machines en réseau qui sont utilisées par des personnes différentes, la deuxième méthode est nettement préférable. En effet, la base de registres Hkey\_Local\_Machine n'est pas enregistrée avec les paramètres de l'utilisateur, si bien que l'information va demeurer dans la machine. Le prochain utilisateur qui va lancer Access sera d'emblée connecté au dernier groupe de travail utilisé et non pas au groupe de travail par défaut !

Remarque : Dans Microsoft Access 97, les préférences utilisateur sont stockées dans la base de registres Windows sous la clé :

Hkey\_Current\_User\Software\Microsoft\Office\8.0\Access\Settings.

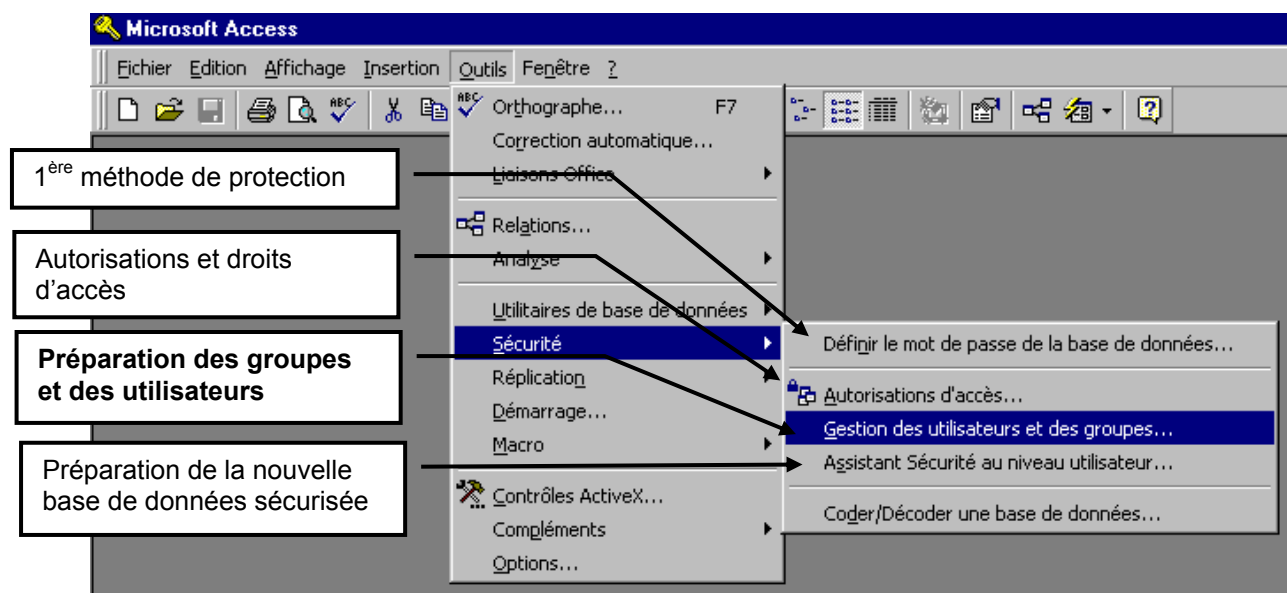
### Organisation du nouvel espace de travail

Maintenant que l'espace de travail est créé, il faut s'occuper de l'organiser :

- Définir les différents groupes d'utilisateurs
- Identifier les différents « comptes » utilisateurs
- Attribuer les utilisateurs à un ou plusieurs groupes.

Ces différentes opérations s'effectuent **dans ACCESS**, une fois que l'on est « connecté » au groupe de travail désiré !

C'est le Menu « Outils » qui donne accès aux options « **Sécurité** ».



Rappel : Lorsque l'on crée pour la première fois un fichier d'information de groupe de travail, on est considéré par le système comme étant le fameux « Administrateur » qui dispose de tous les droits. Il faut user de ces droits avec discernement et agir avec méthode pour ne pas se trouver « coincé » par une mauvaise manipulation.

**1<sup>ère</sup> opération : créer un nouvel Administrateur**, différent de l'administrateur par défaut !

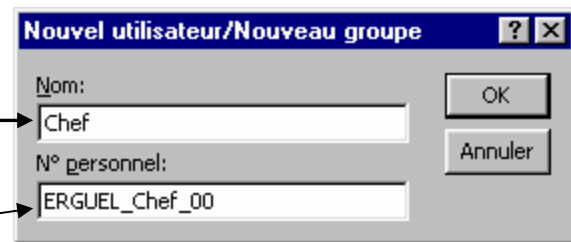
1° Créer le nouvel Administrateur

Choisir un nom symbolique du genre :

BigBoss, Patron, Chef, etc.

Ou utiliser le nom du véritable administrateur du groupe de travail :

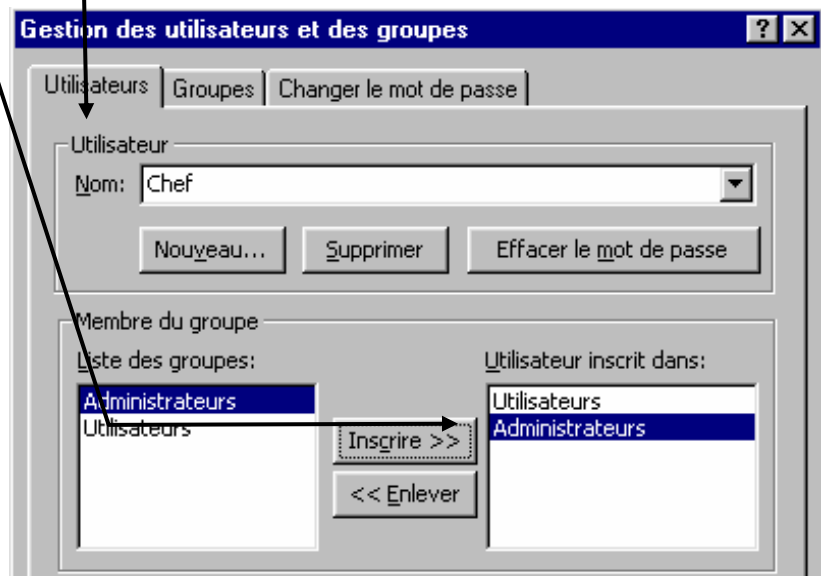
John, Claudia, K\_Ribou, etc.



Le N° personnel permet de distinguer des utilisateurs qui auraient le même nom. Comme on l'a déjà vu au chapitre 3, Il faut conserver cette information dans un endroit sûr, pour le cas où il faudrait re-crée le fichier d'information du groupe de travail ainsi que les utilisateurs qui le composent !

2° Incrire absolument cet utilisateur dans le groupe des Administrateurs !

En prévision du point 3°, il est indispensable qu'une personne au moins soit membre du groupe « Administrateurs » pour disposer des pouvoirs nécessaires à la poursuite des opérations !

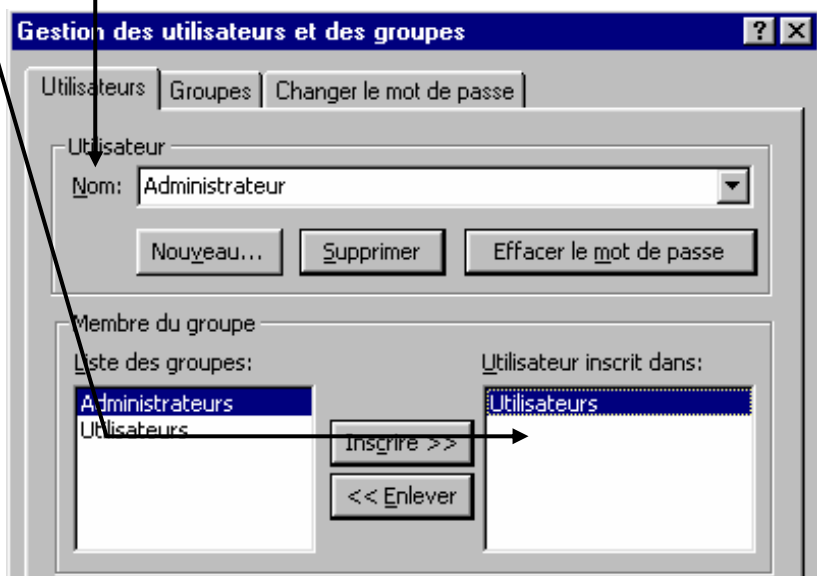


3° Retirer l'ancien Administrateur » du groupe « Administrateurs ».

De cette manière, les éventuels « Administrateurs » d'autres groupes de travail ne pourront plus jamais prendre possession des bases de données qui vont être créées par le nouveau groupe de travail.

4° Donner un mot de passe à cet ancien « Administrateur ».

Il n'est pas possible de détruire ce compte ( ? ! ) qui va demeurer en tant qu'utilisateur. Il faut donc empêcher que n'importe qui puisse accéder, sans contrôle, à ce groupe de travail en utilisant le nom « Administrateur ».



5° Quitter ACCESS.

6° Relancer ACCESS.

Cette fois, une boîte de dialogue « Connexion » doit apparaître...

Il faut saisir ou sélectionner le nouvel « Administrateur ».

Il n'a pas encore de mot de passe ...

7° Attribuer un mot de passe à l'Administrateur, puisque l'on est connecté sous son nom.

Rien ici, car il n'y a pas encore de mot de passe

Rappel :  
Les mots de passe sont  
« case sensitive » ! ! !

## 2<sup>ème</sup> opération : créer les groupes d'utilisateurs.

Par exemple : Membres  
Comité  
Etc

Selon la structure et les besoins de l'entreprise...

## 3<sup>ème</sup> opération : créer les comptes d'utilisateurs.

Le terme « compte d'utilisateur » provient du début de l'informatique, lorsque l'on tenait le **compte** du temps que chaque utilisateur passait sur son terminal connecté sur l'ordinateur central en « time sharing ».

## 4<sup>ème</sup> opération : attribuer les utilisateurs aux différents groupes.

L'avantage des groupes, c'est qu'en attribuant un utilisateur à l'un d'entre eux, cet utilisateur acquiert d'un seul coup tous les droits et toutes les autorisations que l'on a accordés à ce groupe au préalable.

Il n'y a donc pas besoin de définir individuellement le détail des droits de chaque utilisateur : il suffit de le prévoir pour son groupe et de lui faire rejoindre ce groupe !

Droits et autorisations seront traités au chapitre 7.

**Bases de données et espace de travail**

Maintenant que l'espace de travail est délimité, il faut encore y incorporer les bases de données que les utilisateurs vont utiliser ! Deux cas de figure non exclusifs peuvent se présenter :

- On veut créer de nouvelles bases de données à partir de l'espace de travail choisi.
- On veut utiliser, en les sécurisant dans cet espace de travail, des bases de données existantes.

Dans les deux cas pourtant la procédure est la même : il faut **faire une copie** de la base de données existante en la passant par une « moulinette » particulière : un « Assistant sécurité » !

## Créer une nouvelle base de données

Il faut créer une base de données en suivant le processus habituel de création :

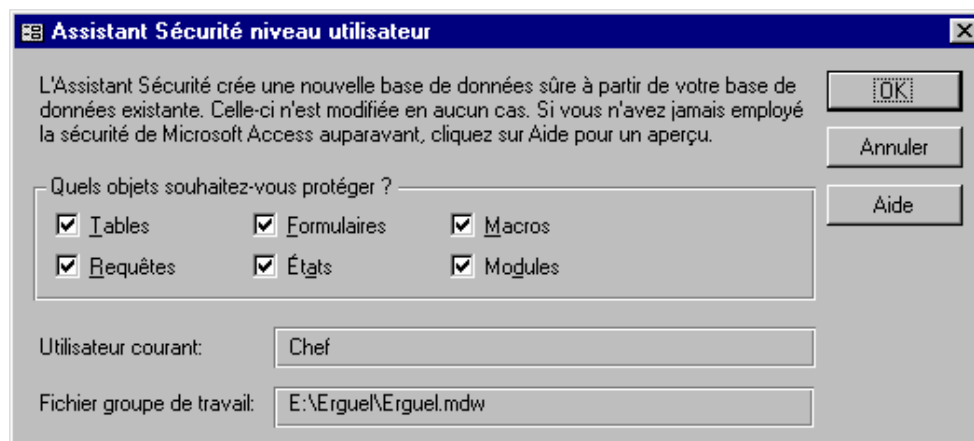
Menu « Fichiers » - « Nouvelle base de données » - « Base de données vide ».

On se contentera de lui attribuer le nom proposé par défaut, « Bd1.mdb », car on a seulement besoin d'une boîte vide pour la suite des opérations...



## Sécuriser une base de données existante

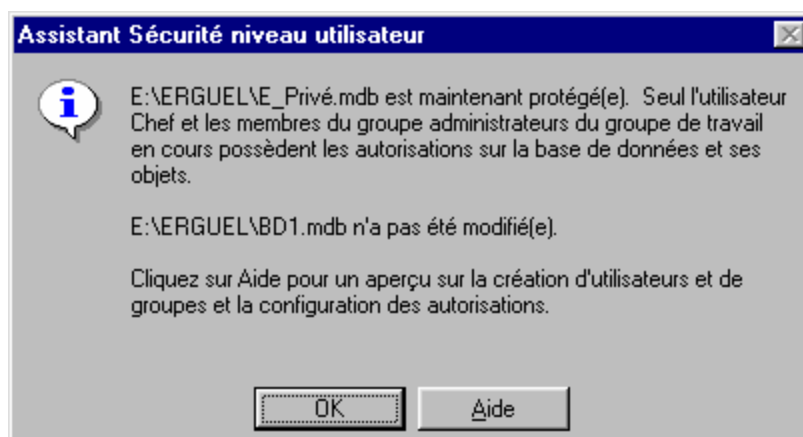
- 1° Se connecter à l'espace de travail en tant qu' « Administrateur ».
- 2° Ouvrir la base de données (pleine ou vide).
- 3° Menu « Outils » - « Sécurité » - « Assistant sécurité au niveau utilisateur ».



- 4° Indiquer le nouveau nom de la base de données, l'unité et le répertoire de destination...

- 5° La base ainsi créée est la « propriété » de l' « Administrateur » :

tant qu'il n'aura pas déterminé les droits d'accès, nul autre ne sera autorisé à pénétrer et, à plus forte raison, à utiliser cette base de données.



## Autorisations et droits d'accès

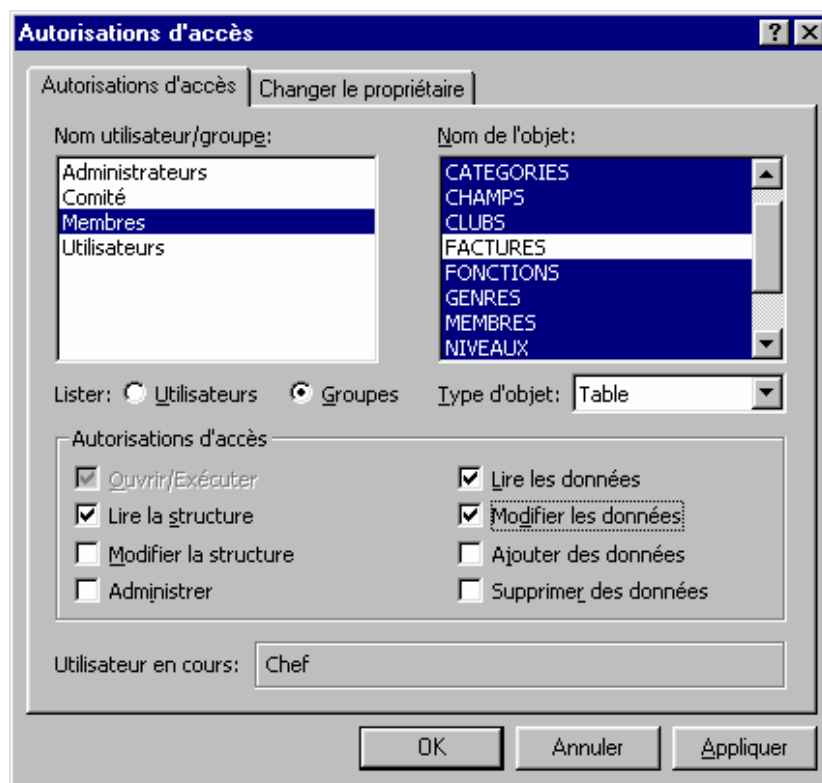
Si l'on veut gérer correctement une base de données sécurisée, il faut déterminer pour chaque utilisateur et pour chaque groupe quels sont leurs droits précis sur chaque objet de la base !

La meilleure méthode est de définir les droits et les autorisations pour un groupe, d'assigner un utilisateur à ce groupe et de tester si les manipulations des données nécessaires sont toutes possibles pour cet utilisateur. En cas de problèmes, modifier les autorisations du groupe. Quand tout fonctionne, tous les autres utilisateurs assignés à ce groupe pourront travailler sans soucis.

- 1° Menu « Outils » - « Sécurité » - « Autorisation d'accès »
- 2° Dans l'onglet « Autorisations d'accès », choisir Groupes (ou Utilisateurs), puis le groupe (ou l'utilisateur) auquel on souhaite accorder les autorisations d'accès.
- 3° Cliquer sur le type d'objet dans la boîte Type de l'objet, puis sur le nom de l'objet auquel les autorisations d'accès se rapporteront dans la boîte Nom de l'objet.

Conseil : On peut sélectionner plusieurs objets dans la boîte Nom de l'objet en faisant glisser le pointeur de la souris sur les objets que l'on veut sélectionner ou en maintenant la touche CTRL enfoncée et en cliquant sur les objets souhaités.

- 4° Dans Autorisations d'accès, sélectionner les autorisations d'accès que l'on veut accorder, ou effacer les autorisations d'accès que l'on veut retirer au groupe ou à l'utilisateur, puis cliquer sur **Appliquer**.



Répéter les étapes 4 et 5 pour accorder ou retirer au groupe (ou à l'utilisateur) en cours d'autres autorisations d'accès portant sur d'autres objets.

## Remarques

- Certaines autorisations d'accès s'accompagnent automatiquement de la sélection d'autres autorisations d'accès. Par exemple, l'autorisation d'accès « Modifier les données » d'une table



s'accompagne automatiquement des autorisations d'accès « Lire les données » et « Lire la structure », car on en a besoin pour modifier les données d'une table.

« Lire les données » s'accompagnent automatiquement de « Lire la structure ». Dans le cas des macros, « Lire la structure » s'accompagne automatiquement de « Ouvrir/Exécuter ».

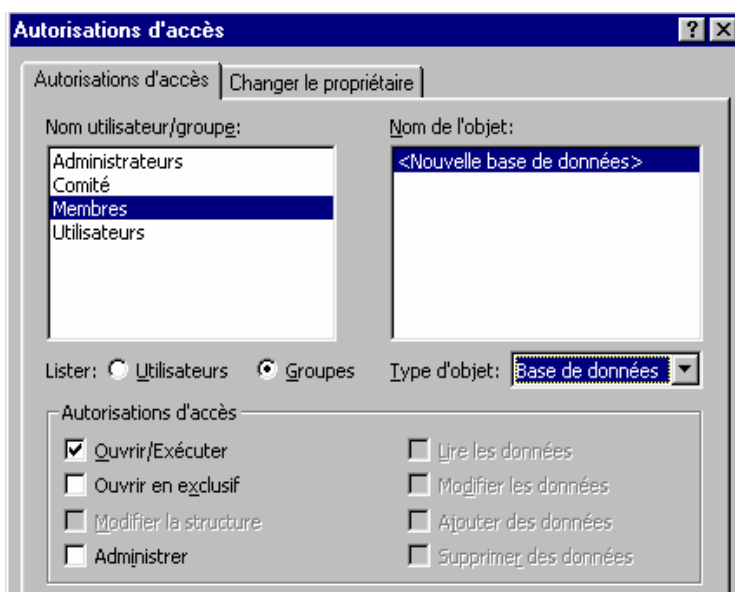
- Lorsque l'on modifie un objet et qu'on l'enregistre, il conserve les autorisations d'accès qui lui sont accordées.
- Toutefois, si un objet est enregistré sous un nouveau nom à l'aide de la commande Enregistrer sous dans le menu Fichier, ou en coupant et en collant, en important ou en exportant l'objet, les autorisations d'accès associées sont perdues ! Il faut les accorder à nouveau.

#### Types d'autorisations d'accès

Autorisation	Permet à un utilisateur de	S'applique à
Ouvrir/exécuter	Ouvrir une base de données, un formulaire ou un état, ou exécuter une macro.	Bases de données, formulaires, états et macros
Ouvrir en mode exclusif	Ouvrir une base de données avec accès exclusif.	Bases de données
Lire la structure	Afficher des objets en mode Création.	Tables, requêtes, formulaires, états, macros et modules
Modifier la structure	Afficher et modifier les objets, ou les effacer.	Tables, requêtes, formulaires, états, macros et modules
Lire les données	Afficher des données.	Tables et requêtes
Modifier les données	Afficher et modifier des données, sans pouvoir en ajouter ou en supprimer.	Tables et requêtes
Ajouter des données	Afficher et ajouter des données, sans pouvoir en modifier ou en supprimer.	Tables et requêtes
Supprimer des données	Afficher et supprimer des données, sans pouvoir en modifier ou en ajouter.	Tables et requêtes
Administrer	Définir un mot de passe pour une base de données, copier une base de données et modifier les propriétés de démarrage	

#### Ne pas oublier ...

- D'**enlever** systématiquement toute autorisation de chaque objet de la base de données (Tables, Requêtes, Formulaires, Macros, etc) pour le groupe « Utilisateurs » si on n'utilise pas !
- D'**accorder** l'autorisation « Ouvrir/Exécuter » à l'objet « Nouvelle base de données » à **chaque groupe**, de telle manière que ses membres puissent ... ouvrir la base dans laquelle ils vont travailler !



## Connexion à une base de données sécurisée

La connexion réclame plusieurs conditions :

- 1° Faire partie de l'espace de travail
- 2° Fournir son nom d'utilisateur
- 3° Eventuellement, fournir le nom de la base de données que l'on veut utiliser.

Il est possible d'automatiser cette procédure pour un utilisateur particulier au moyen d'un raccourci sur le bureau ou dans la barres des tâches.

Exemple 1 : Choix de l'espace de travail et indication du nom de l'utilisateur

F:\MsOffice\Office\Msaccess.exe /wrkgrp G:\Erguel\Erguel.mdw /user Chef

Programme Access      Groupe de travail      Utilisateur

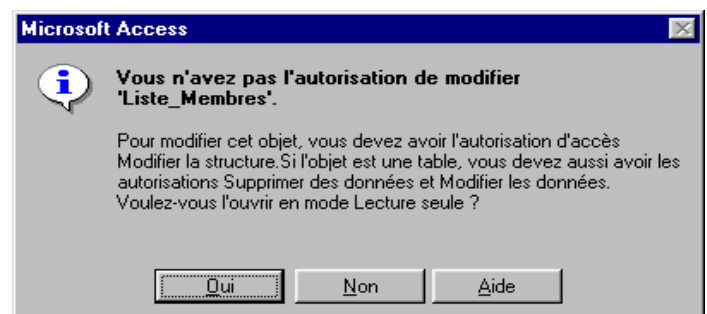
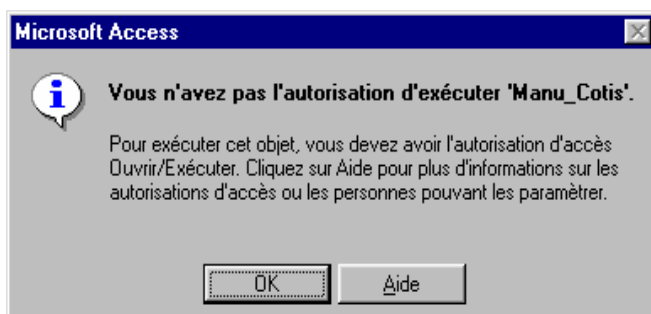
Exemple 2 : Idem + indication de la base de données

F:\MsOffice\Office\Msaccess.exe G:\Ecole\Ecole.mdb /wrkgrp G:\Ecole\System.mdw /user Bigboss

Programme Access      Base      Groupe de travail      Utilisateur

## Prise en compte des autorisations

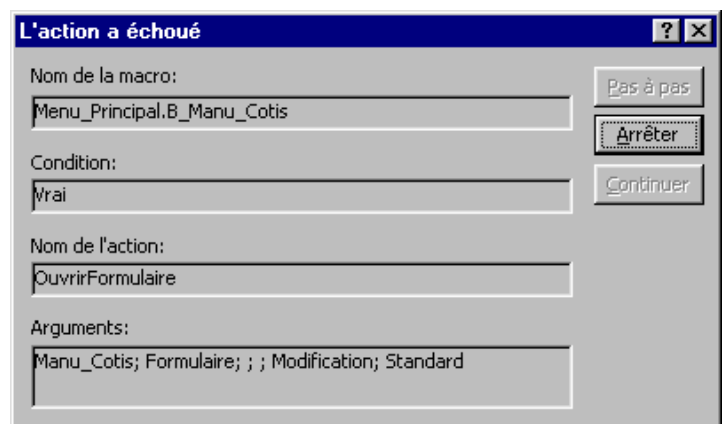
Lorsqu'un utilisateur tente d'ouvrir, de modifier ou de détruire un objet auquel il n'a pas accès, il reçoit un message lui signifiant son éviction :



Cependant, lorsque cet utilisateur clique sur un **bouton** qui le conduit dans un domaine auquel il n'a pas accès, le résultat n'est pas très heureux si l'action est mise en oeuvre par une **macro** :

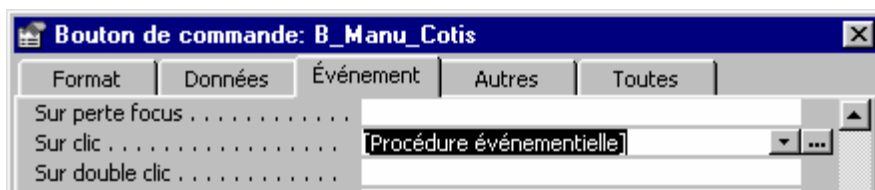
Le message apparaît ...

... Et la macro se plante !



En conséquence, il vaut mieux être méthodique et respecter cette consigne :

Dans une base de données sécurisée, les actions des **boutons** doivent être générées par une **procédure événementielle** qui comporte un **traitement des erreurs** !



Exemple :

```
Private Sub B_Manu_Cotis_Click()

    On Error GoTo Err_B_Manu_Cotis_Click

    DoCmd.OpenForm "MANU_COTIS"

Exit_B_Manu_Cotis_Click:

    Exit Sub

Err_B_Manu_Cotis_Click:

    MsgBox Error$

    Resume Exit_B_Manu_Cotis_Click

End Sub
```

L'utilisateur a le droit  
d'accès :  
Ouverture normale

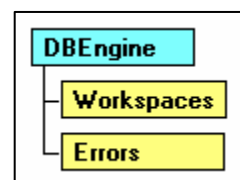
Pas de droit d'accès :  
Message d'erreur et sortie

### La sécurité dans Visual Basic pour Access

L'environnement ACCESS est structuré en « Objets » et en « Collections d'objets ».

L'objet originel et unique est « DBEngine », le « moteur » du système de gestion de base de données, c'est à dire l'ensemble des programmes qui contrôle tout le processus.

Ce moteur contrôle deux collections (ou ensembles) d'objets : les « Espaces de travail » et la liste des erreurs.

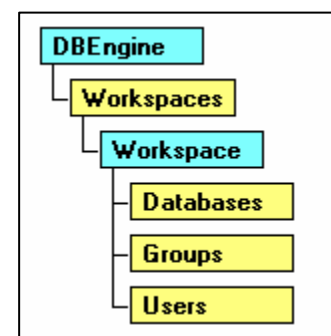


On voit donc que le terme « Espace de travail » est le mot générique et que la traduction en « Groupe de travail » est un peu confondante.

Le moteur permet de gérer les différents « Espaces de travail ».

Chaque espace de travail peut contenir un certain nombre de groupes d'objets :

- Databases : une ou plusieurs Bases de données
- Groups : un ou plusieurs Groupes
- Users : un ou plusieurs Utilisateurs.



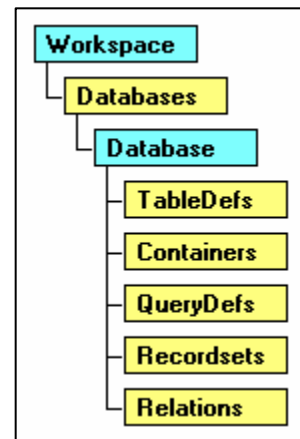
Groups et Users sont complémentaires :

Chaque groupe peut compter un ou plusieurs utilisateurs  
Chaque utilisateur peut faire partie de plusieurs groupes.

Pour compléter cette information, on voit qu'une Base de données est composée de collections d'objets très bien organisés :

- TableDefs : les descriptions de toutes les tables et de toutes les propriétés de tous leurs champs.
- Recordsets : tous les enregistrements de toutes les tables
- Relations : les descriptions de toutes les relations existant entre toutes les tables
- QueryDefs : les descriptions de toutes les requêtes
- Containers : les descriptions de tous les formulaires et états.

Visual Basic pour Access permet de traiter tous les objets de toutes les manières possibles : création, modification, suppression !



VBA offre une systématique remarquable pour :

- **Désigner** chaque objet
- Modifier ses **propriétés**
- Exécuter ses **méthodes**.

Avant de passer en revue les **propriétés** et les **méthodes** de tous ces objets, il faut tout d'abord s'occuper de deux besoins élémentaires pour la gestion des droits d'accès :

- Obtenir le **nom** de l'utilisateur courant
- Obtenir le **groupe** auquel appartient cet utilisateur.

## Obtenir le nom de l'utilisateur courant

```
Function QuelUser()  
  
    Dim Espace As Workspace  
    Set Espace = DBEngine.Workspaces(0)  
    QuelUser = Espace.UserName  
    Set Espace = Nothing  
  
End Function
```

## Obtenir le groupe de l'utilisateur courant (à part Admins et Users)

```
Function QuelGroupe()  
  
    Dim Espace As Workspace  
    Dim Branché As USER  
    Dim LeGroupe As Group  
  
    Set Espace = DBEngine.Workspaces(0)  
    Set Branché = Espace.USERS(Espace.UserName)  
    For Each LeGroupe In Branché.Groups  
        If LeGroupe.Name = "Admins" Or LeGroupe.Name = "Users" Then  
            Else  
                QuelGroupe = LeGroupe.Name  
            End If  
    Next LeGroupe  
    Set Espace = Nothing  
  
End Function
```