LA GESTION DE LA SÉCURITÉ ET DES ACCÈS DANS MAESTRO*

S'il est un aspect où Maestro ne lésine pas, c'est bien la sécurité! En effet, tout progiciel de gestion intégré met en commun et travaille avec nombre de données confidentielles. Si certaines de ces données peuvent être partagées à des utilisateurs clés, d'autres, par contre, doivent être restreintes à seuls quelques utilisateurs. Pour répondre aux besoins de gestion de sécurité nombreux et variés de ses clients, **maestro*** offre une multitude de fonctionnalités vouées à cet effet.

SOMMAIRE

Profil de sécurité basé sur l'utilisateur

En premier lieu, chaque employé appelé à travailler avec **maestro*** doit se voir créer un profil d'utilisateur. Divers accès et paramètres de sécurité sont rattachés à ce profil, faisant en sorte que ce premier niveau de sécurité est attribué sur une base individuelle.

L'administrateur de maestro*

Chaque entreprise doit d'abord désigner un ou plusieurs administrateur(s) **maestro***. Un administrateur possède en fait tous les droits et accès dans le progiciel. C'est cette personne qui est responsable de créer les profils de sécurité des autres utilisateurs et généralement, c'est elle aussi qui effectue la majorité de configurations dans **maestro***.

Code et numéro d'utilisateur

Chaque nouvel utilisateur de **maestro*** se voit attribuer un code et un numéro d'utilisateur[1] . À l'exception des utilisateurs **de maestro*CLOUD**, pour lesquels le code doit consister en l'adresse courriel, aucune restriction ne s'applique à l'attribution du code d'utilisateur. C'est ce code qui, jumelé à un mot de passe, permettra à l'utilisateur d'accéder à **maestro*** et/ou **maestro*MOBILE**. Le numéro d'utilisateur est, quant à lui, généré par **maestro***. Il ne peut être modifié et il est rattaché aux données proprement dites.

Il est recommandé de ne jamais réutiliser un code d'utilisateur. De plus, le numéro d'utilisateur fait en sorte que l'historique de ce dernier est conservé et que des statistiques peuvent être obtenues quant aux accès effectués.

Mot de passe

Comme tout bon logiciel, l'accès à **maestro*** est protégé par l'utilisation d'un mot de passe. Initialement attribué par l'administrateur, il peut être modifié par l'utilisateur lui-même selon une fréquence prédéterminée et/ou lors de la prochaine connexion de ce dernier.

Prendre note que les mots de passe pour accéder à **maestro*** 3.05 MSSQL doivent respecter les règles que voici :

- Ils doivent compter au moins huit caractères
- Ils doivent contenir des caractères appartenant à trois des quatre catégories suivantes :
  - Lettres majuscules de l'alphabet latin (A à Z)
  - Lettres minuscules de l'alphabet latin (a à z)
  - Chiffres de la base 10 (0 à 9)
  - Caractères non alphanumériques tels que : point d'exclamation (!), symbole dollar ($), signe dièse (#) ou pourcentage (%).

De plus, le code de l'utilisateur ne doit pas être utilisé en guise de mot de passe.

[1] Appelé usager dans maestro*

Il va de soi que les mots de passe pour accéder à **maestro*** ne doivent en aucun cas être partagés. De plus, lors de l'attribution du mot de passe initial et une fois le profil de sécurité d'un nouvel utilisateur créé, l'administrateur de **maestro*** a la possibilité de se connecter tel l'utilisateur configuré afin de vérifier les configurations et les accès de ce dernier.

Pour connaître de bonnes pratiques en matière de mots de passe, consulter l'annexe intitulé ***Bonnes pratiques en matière de gestion des mots de passe***, présenté à la fin de ce document.

Types d'accès

Chaque utilisateur se voit également définir un type d'accès correspondant au(x) produit(s) **maestro*** pour le (s)quel(s) il a accès et au type de connexion utilisé. Un utilisateur peut avoir accès :

- à **maestro*** seulement (par le biais d'une connexion au réseau interne);
- à **maestro*MOBILE** seulement (soit l'application);
- au mode employé de **maestro*MOBILE** (qui permet uniquement de compléter les feuilles de temps à l'aide de l'application **maestro*MOBILE**);
- à **maestro*** et **maestro*MOBILE**;
- à **maestro*CLOUD** (lorsque l'utilisateur accède à **maestro*** par le biais d'un service Web).

Il va de soi que le type d'accès **maestro*** ne donne pas nécessairement accès à l'ensemble des modules, fonctionnalités et données de **maestro***. À la base, seuls les modules achetés par le client sont disponibles et plusieurs autres paramètres interviennent dans l'attribution des accès.

Bien qu'un administrateur puisse créer le nombre d'utilisateurs détenant un accès exclusif à **maestro*** dont il a besoin, le nombre d'utilisateurs de **maestro*MOBILE** est limité au nombre de licences **maestro*MOBILE** acquises par l'entreprise. Il est donc requis de rendre un utilisateur **maestro*MOBILE** inactif ou de procéder à l'achat d'une licence supplémentaire lorsque vient le moment d'attribuer une licence **maestro*MOBILE** à un nouvel employé en ayant besoin.

Sécurité par projets

Toujours sur une base individuelle, **maestro*** permet d'appliquer une sécurité par projets en permettant aux utilisateurs d'accéder aux informations de tous les projets, de projets triés sur le volet ou de projets appartenant à un type ou une catégorie de projets spécifiques.

L'attribution de types et/ou de catégories aux projets facilite la gestion de la sécurité des projets puisqu'elle évite, lors de la création d'un nouveau projet, d'avoir à indiquer pour chacun des utilisateurs de **maestro*** s'ils peuvent ou non accéder aux informations dudit projet.

Encore plus, il est possible d'autoriser ou restreindre la visualisation des montants et/ou des quantités inscrites pour chacun des groupes de revenus et de dépenses de ces projets.

Mentionnons également qu'il est envisageable de restreindre l'accès à chaque compte créé dans la structure comptable par la création de groupes de sécurité puis par l'attribution d'un code de groupe de sécurité à chacun de ces comptes.

Accès aux données des employés

Pour chaque utilisateur, l'administrateur doit spécifier si ce dernier aura accès aux informations de tous les employés, d'aucun, d'un groupe particulier d'employés ou de certains employés seulement. Si un accès à un ou des employés est attribué, il devient nécessaire de préciser si cet accès doit être restreint ou non. Lorsqu'il doit l'être, il est possible de cacher les coordonnées des employés, de permettre ou non l'accès à la gestion des documents et de cacher ou non l'identité des employés (numéro, nom, NAS) et/ou le salaire (taux, montant) dans les rapports et consultations. Aussi, lorsqu'un utilisateur a les droits pour accéder à la **Gestion des employés**, l'administrateur peut décider de n'autoriser la consultation et la modification que de certaines informations seulement. De cette façon, il est possible de faire en sorte que seuls les employés travaillant à la paie aient accès à l'information nécessaire à l'accomplissement de leurs tâches, sans plus.

Accès aux compagnies

Lorsque l'entreprise gère plus d'une compagnie, **maestro*** permet d'identifier celle(s) à laquelle (auxquelles) aura accès l'utilisateur lors de sa connexion au logiciel.

Voir également la section concernant la sécurité appliquée à une compagnie.

Restrictions individuelles

Outre les accès déjà présentés, une panoplie de restrictions peuvent être ajoutées sur une base individuelle :

Par exemple, pour la grande majorité des modules et options de **maestro***, l'administrateur aura la responsabilité d'accorder ou non des droits et restrictions spécifiques qui s'appliqueront:

- aux divers états financiers et rapports;
- aux transferts de transactions;
- à la consultation des informations des équipements, des contrats de service, des soumissions (restrictions appliquées par onglets);
- aux soumissions, avis de changement, commandes, etc., selon leurs états;
- à la visualisation de la profitabilité et des montants des commandes et des ventes;
- à la création de notes de crédit et/ou à la modification des prix d'une commande;
- à la modification des budgets et la visualisation des totaux des projets;
- à la visualisation des prix des soumissions;
- à la confirmation des feuilles de temps et à la modification de celles qui sont transférées;
- à la création et/ou la duplication de rapports et de tableaux de bord dans **maestro*BI**;
- etc.

Dans **maestro***, une fonctionnalité permet également de reproduire les accès de sécurité d'un utilisateur source à un autre. Celle-ci est fort utilisée, entre autres, lorsque des employés ont un poste et/ou des fonctions similaires; par exemple des employés du Département des comptes payables. En effet, il est beaucoup plus rapide et sûr de copier un profil de sécurité existant, quitte à effectuer quelques modifications a posteriori, que de réaliser individuellement le profil de sécurité de chaque utilisateur si ces derniers s'avèrent quasi identiques. Cette fonctionnalité est également utilisée lors des départs et arrivées d'employés, afin de reproduire des profils de sécurité semblables. Enfin, il est également possible de copier les paramètres d'affichage, par exemple les colonnes visibles d'une grille, d'un employé à l'autre.

Protection des documents et des courriels

Dans **maestro***, on appelle contact toute entité avec laquelle une entreprise peut être appelée à transiger, à communiquer et pour laquelle on souhaite répertorier entre autres les coordonnées. Ces contacts peuvent consister en des individus, en des compagnies ou encore, en des emplacements. On trouvera donc dans les contacts de **maestro*** des employés et utilisateurs, des clients, des fournisseurs, des sous-traitants, etc.

Pour chacun de ces contacts, il est possible d'indiquer un mot de passe qui sera requis pour l'ouverture des documents envoyés par courriel, à partir des envois massifs. Cette fonctionnalité est particulièrement intéressante lorsque vient le moment d'envoyer les talons de paie aux employés!

Bref, **maestro*** offre énormément de précision lorsque vient le temps d'attribuer ou non les accès par individu.

Authentification multifacteur pour les utilisateurs de maestro*CLOUD

De nos jours, l'authentification avec un seul mot de passe est devenue insuffisante. Les clients qui bénéficient de l'installation de la suite *Office* de *Microsoft* sur leurs postes de travail sont pourvus d'un accès de type **Authentification multifacteur**, connu sous l'appellation anglaise *Multi-Factor Authentication* (MFA). Le MFA permet d'authentifier une personne par au moins 2 facteurs parmi les 3 suivants :

- quelque chose que la personne connaît (généralement un mot de passe);
- quelque chose qu'elle possède (souvent un téléphone);
- ou quelque chose qu'elle "est" (en utilisant la biométrie).

Or, l'utilisation de **maestro*CLOUD** fait en sorte que les clients ne transigent pas à partir d'*Office* mais utilisent plutôt le protocole de communication SMTP pour transférer le courrier électronique en provenance de **maestro*** vers un serveur de messagerie électronique, et vice-versa. Fait important, l'utilisation de SMTP nécessite que l'authentification multifacteur soit activée pour que seuls les sites reconnus soient autorisés à transmettre des courriels par *Office 365*. Pour bénéficier d'une authentification multifacteur avec SMTP, Maestro propose donc à ses clients **maestro*CLOUD** deux alternatives, la principale consistant en génération, dans *Office 365*, d'un mot de passe spécial concernant l'accès à *Office 365* puis, à la configuration de ce mot de passe dans **maestro***. Pour en savoir davantage sur le sujet, consulter le document intitulé Office 365, Authentification multifacteur et maestro*.

Profil de sécurité basé sur un groupe d'utilisateurs

En sus du profil de sécurité individuel d'un utilisateur, s'ajoute le profil de sécurité du groupe d'utilisateurs auquel appartient ce dernier. L'attribution d'un groupe d'utilisateurs est obligatoire pour tout utilisateur créé dans **maestro***. Cela fait en sorte qu'un deuxième niveau de sécurité s'ajoute au premier. Il vient ainsi limiter, entre autres, l'accès aux modules et aux options de **maestro***. Ces restrictions s'appliquent à tous les utilisateurs faisant partie du groupe. Lorsqu'un changement est effectué au niveau de la sécurité du groupe d'utilisateurs, tous les utilisateurs faisant partie du groupe sont impactés.

Un groupe d'utilisateurs, dans **maestro***, peut donc être défini comme un groupe d'employés au profil et/ou fonction(s) similaire(s). Les groupes d'utilisateurs sont créés selon la taille, la composition d'employés et les besoins de l'entreprise. Il pourrait s'agir, par exemple, des groupes suivants : *direction*, *employés réguliers sans accès à la paie*, *employés réguliers avec accès à la paie*, *chargés de projet*, *techniciens mobile*, *administration*, etc. Pour chacun des groupes d'utilisateurs créés, l'administrateur devra définir les types de sécurité, le niveau d'accès et l'accès aux modules. C'est également l'administrateur qui décide du nombre de groupes d'utilisateurs à créer et nécessaire à la gestion optimale de la sécurité pour la compagnie.

Un utilisateur ne peut être rattaché qu'à un seul groupe d'utilisateurs.

Niveaux d'accès

Chaque groupe d'utilisateurs se voit aussi attribuer l'un des niveaux d'accès possibles dans **maestro*** qui, selon l'installation effectuée, peut être *administrateur*, *administrateur local*, *régulier*, *employé* ***maestro*MOBILE*** ou technique.

Tel que mentionné précédemment, l'administrateur de **maestro***, soit un utilisateur principal ou en chef, détient les accès à tous les modules achetés par l'entreprise. C'est cette personne qui est responsable de l'octroi des droits d'accès dans **maestro*** et des configurations liées à la sécurité. C'est à cette personne qu'est attribué le niveau d'accès *administrateur*. Un *administrateur local*, quant à lui, a aussi tous les droits mais ceux-ci sont limités à (aux) la compagnie(s) à laquelle (auxquelles) il a accès (voir la section concernant la sécurité par domaine). Les employés qui n'ont accès qu'à **maestro*MOBILE** pour compléter leurs feuilles de temps doivent détenir un niveau d'accès de type *employé* ***maestro*MOBILE*** alors que tous les autres employés se voient décernés le niveau *régulier*, correspondant à des accès configurés sur mesure. Enfin, le niveau *technique* est réservé aux techniciens qui effectuent entre autres le support technique et, s'il y a lieu, les sauvegardes et les mises à jour de **maestro***. Ce dernier niveau leur permet d'accéder à **maestro*** pour vérifier que tout est fonctionnel sans pour autant visualiser des données dites sensibles (par exemple les données financières de l'entreprise).

Accès aux modules

Outre les choix de donner aux groupes d'utilisateurs la possibilité de voir ou non les options qui leur sont permises et la possibilité d'accéder à ces options pour voir l'information seulement ou pour pouvoir l'insérer, la modifier et la supprimer, **maestro*** permet de cocher spécifiquement chaque option, groupe d'options, sous-

module et/ou module au(x)quel(s) aura accès un groupe d'utilisateurs donné. Ainsi, il est possible d'afficher le module **Paie** dans le menu de **maestro*** seulement pour le groupe d'employés travaillant à la paie et pour l'administrateur. De la même façon, il est possible de restreindre l'accès et la vue de certaines options du module **Comptabilité** pour la majorité des groupes d'utilisateurs et de limiter l'accès à chaque compte créé dans la structure comptable par la création de groupes de sécurité puis par l'attribution d'un code de groupe de sécurité à chacun de ces comptes.

Sécurité appliquée à une compagnie

Outre la sécurité individuelle et par groupe d'utilisateurs, des fonctionnalités permettent également d'appliquer des mesures au niveau des compagnies en elles-mêmes.

Types de sécurité

Maestro* permet de spécifier si la sécurité doit être :

- globale; ou
- locale.

Lorsque la sécurité de **maestro*** est globale, cela signifie que les configurations de sécurité s'appliquent à toutes les compagnies du client (incluant la compagnie test). En contrepartie, une sécurité locale fait en sorte que les configurations de sécurité ne s'appliquent qu'à la compagnie en cours d'utilisation. En effet, et dans le cas où un client détient plus d'une compagnie, il peut être souhaité qu'une sécurité différente s'applique, selon la compagnie. Un autre client peut souhaiter à l'inverse, par exemple, que les mêmes restrictions s'appliquent d'une compagnie à l'autre. De plus, lorsque la sécurité est appliquée globalement, toute modification à celle-ci se répercute dans les autres compagnies. Il s'agit du type de sécurité recommandé par Maestro pour la grande majorité des entreprises.

Tout changement à la sécurité effectué dans une compagnie test affectera également les autres compagnies où la sécurité est globale.

Toutes les entreprises travaillant avec **maestro*** se voient créer, lors du *go-live*, une compagnie test. Celle-ci se veut une réplique de la compagnie réelle utilisée par l'entreprise dans **maestro***. La compagnie test permet, comme son nom l'indique, de tester, de former de nouveaux utilisateurs sur **maestro***, etc. Toutes les transactions réalisées dans la compagnie test sont fictives.

La sécurité par domaine

La sécurité par domaine peut s'appliquer lorsqu'une entreprise détient plus d'une compagnie ou division. Elle consiste à contrôler l'accès à **maestro*** par groupe de compagnies et à restreindre les accès de certains employés, groupes d'utilisateurs ou utilisateurs administrateurs aux compagnies appartenant à un même groupe de compagnies. Qui plus est, la sécurité par domaine permet de limiter l'accès à des données spécifiques à un ou des domaine(s), de la même façon que **maestro*** permet de restreindre l'accès à des options par groupes d'utilisateurs.

La sécurité par domaine offre la possibilité d'ajouter un nouveau niveau d'accès administrateur : l'administrateur local, aussi appelé administrateur adjoint. Les utilisateurs ayant ce niveau de sécurité ont des droits similaires à ceux d'un administrateur mais ils sont limités aux compagnies faisant partie du domaine identifié dans leur groupe d'utilisateurs. Ceci permet à l'administrateur régulier de **maestro*** de déléguer la gestion de la sécurité à des responsables déterminés pour chaque domaine, sans que ces responsables ne puissent avoir accès aux compagnies qui ne font pas partie du domaine dont ils sont responsables. Ainsi, chaque domaine dispose de paramètres de sécurité qui lui sont propres et fait en sorte, par exemple, qu'un vice-président des finances peut avoir accès à l'information de l'ensemble des compagnies alors qu'un directeur des finances est limité à celle des compagnies figurant dans son domaine.

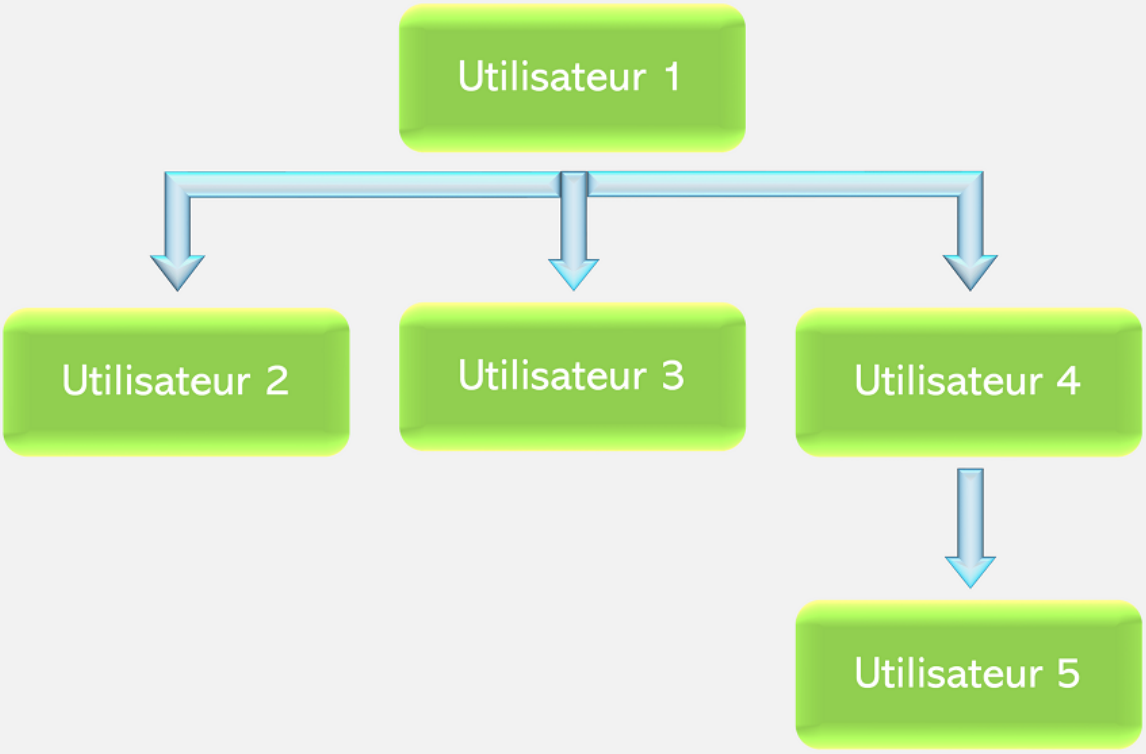
La sécurité par domaine est parfois utilisée lorsque des compagnies sont gérées en mode multidimensionnel.

Utilisateur responsable et modification des transactions

Lorsque désiré, il est possible d'assigner à tout utilisateur de **maestro*** un *utilisateur responsable*. Cet utilisateur responsable peut, au besoin, modifier les transactions de l'utilisateur dont il est responsable. En effet, que ce soit en raison de l'horaire de travail, d'un congé de maladie imprévu, de vacances estivales ou d'une erreur commise, un employé peut être appelé à apporter des modifications à une transaction existante, et ce, même s'il n'en est pas l'initiateur.

Lorsqu'un responsable est identifié pour un utilisateur, le responsable peut modifier les transactions de l'utilisateur mais ce droit est généralement à sens unique. En effet, dans plusieurs cas, le responsable représente un supérieur hiérarchique qui peut avoir, à l'occasion, à modifier une transaction existante initiée par un de ses employés. Il va de soi qu'il ne souhaite pas, en revanche, que ses employés modifient ses propres transactions.

Exemple d'une responsabilité appliquée hiérarchiquement

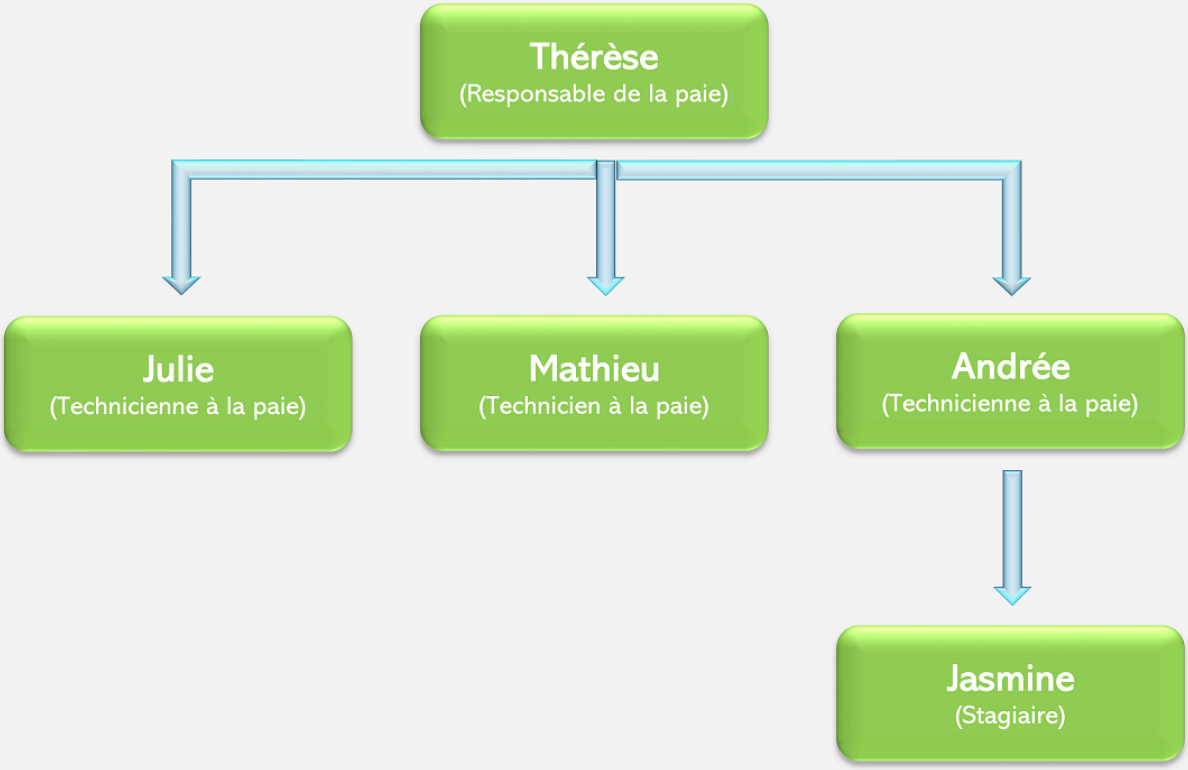


Dans cet exemple, l'utilisateur 1 est le responsable direct des utilisateurs 2, 3 et 4 et il lui est possible de modifier leurs transactions.

L'utilisateur 4 est le responsable direct de l'utilisateur 5 et peut donc modifier les transactions de ce cinquième utilisateur. De ce fait, l'utilisateur 1 devient également responsable de l'utilisateur 5 et peut, lui aussi, modifier les transactions de ce dernier.

À l'exception des utilisateurs 1 et 4, aucun autre ne peut modifier des transactions dont il n'est pas l'auteur.

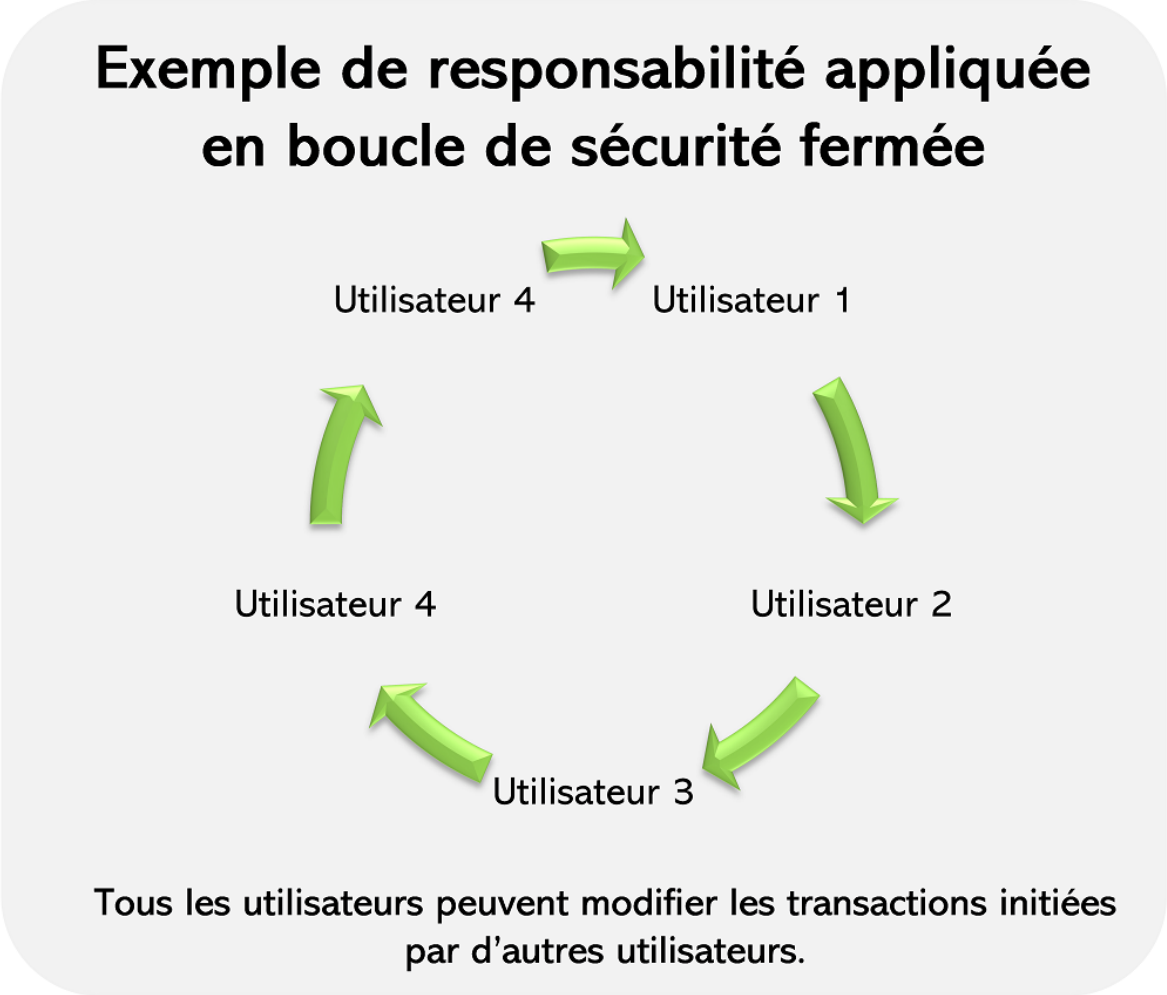
Responsabilité appliquée hiérarchiquement au sein du Département de la paie chez *Marteaux et Cie*



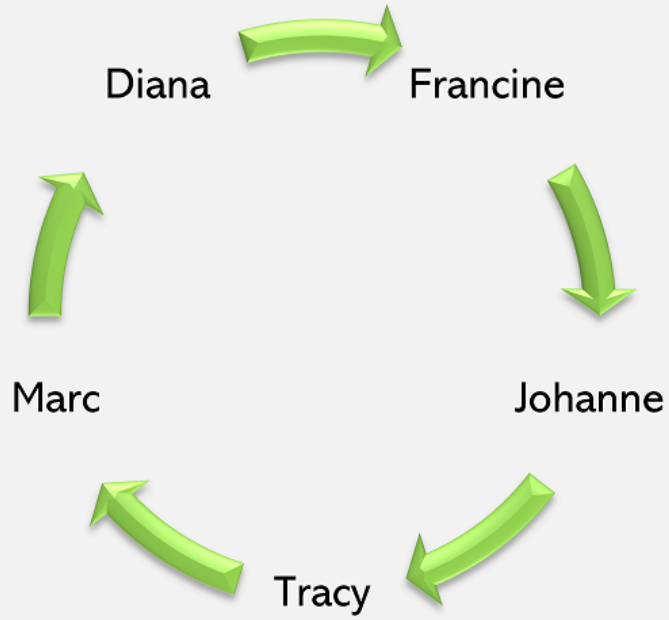
Toujours chez *Marteaux et Cie*, on a décidé d'instaurer la responsabilité hiérarchiquement au sein du **Département de la paie**. Pourquoi? Comme les employés travaillent avec des données sensibles et confidentielles, il est souhaité que seule Thérèse, responsable de la paie, puisse visualiser l'ensemble des salaires des employés et effectuer des modifications, au besoin. Comme Andrée compte énormément d'expérience dans le domaine et que l'on souhaitait lui attribuer davantage de responsabilités, la supervision de Jasmine, stagiaire pour l'été, lui a été confiée. Ainsi, Andrée et Thérèse ont la possibilité d'apporter des correctifs à son travail s'il y a lieu. Autrement, chaque employé du département gère ses propres dossiers.

Il existe tout de même des équipes et/ou circonstances où il est souhaité que des utilisateurs puissent modifier des transactions entre eux et agissent tous à titre de responsable des uns et des autres. On retrouve

fréquemment ce qui est aussi appelé « boucle de sécurité ou de responsabilité fermée » dans les équipes où tous les employés exercent une même fonction ou ont des tâches similaires. Tous les individus du groupe partagent donc les mêmes droits lorsque vient le temps de modifier la transaction d'un pair, faisant partie de ce groupe (ou de cette boucle de sécurité).



Exemple de sécurité en boucle fermée pour les Comptes à recevoir chez *Marteaux et Cie*



L'entreprise *Marteaux et Cie* est une compagnie d'envergure œuvrant dans la construction/rénovation commerciale et industrielle. L'équipe des **Comptes à recevoir** est composée de cinq employés : Francine et Johanne, qui travaillent trois jours par semaine, Tracy et Marc, qui occupent un poste à temps plein, ainsi que Diana, engagée pour un stage de trois mois.

Ces employés ont des tâches identiques et se partagent l'ensemble des dossiers. Comme Marc, Tracy et Diana peuvent être appelés à modifier des transactions initiées par Francine et Johanne, qui travaillent à temps partiel, et comme le travail de stagiaire est sujet à être vérifié et modifié, il a été décidé que les **Comptes à recevoir** de l'entreprise travailleraient en boucle fermée. Cette boucle a également pour effet de faciliter le travail lors de périodes de vacances ou lorsque des employés s'absentent une journée pour cause de maladie.

Restrictions financières

Au-delà des restrictions applicables sur une base individuelle, quant à la vue et la modification de montants et de prix, **maestro*** dispose de fonctionnalités qui permettent un certain contrôle additionnel.

Processus d'approbation

Dans **maestro***, une fonctionnalité appelée **Gestion des processus** permet de mettre en place divers mécanismes pour obtenir l'approbation et alerter certains acteurs clés. Cette option permet d'envoyer un courriel ou un message texte à un ou plusieurs destinataires spécifiques à propos d'une opération précise, par exemple pour la réception de marchandise de plus de 50 000 $. De nombreux cas de figure peuvent être configurés afin de répondre adéquatement à vos besoins.

Accès à Guide

Guide est un portail Web destiné à l'ensemble des utilisateurs de **maestro*** et **maestro*MOBILE**. Le portail permet entre autres d'accéder aux mises à jour de **maestro***, de créer un ticket pour obtenir de l'aide du Support logiciel de Maestro mais surtout, de se voir proposer et/ou de consulter la documentation **maestro*** (comment faire, références techniques, **maestro*EXPRESS**, etc.) mise à la disposition des clients pour solutionner des problématiques ou erreurs encourues avec le logiciel. Un identifiant et un mot de passe propres à l'utilisateur sont nécessaires pour y accéder et déterminent le type d'accès détenu. Ceux-ci sont attribués par l'équipe du Support logiciel.

Niveau de privilège	**Accès et restrictions**
Utilisateur	Le niveau *Utilisateur* permet la consultation des différentes rubriques et documents dans **Guide**. C'est le niveau attribué à la majorité des utilisateurs de **maestro*** et **maestro*MOBILE**. Les utilisateurs de niveau *Utilisateur* ne sont pas autorisés à créer des tickets, à en effectuer le suivi, à contacter le Support logiciel de Maestro ou à télécharger des mises à jour.
Assistant - Tickets Assistant - Mises à jour Assistant - Tickets et mises à jour	Le niveau *Assistant* permet de consulter la documentation mais aussi d'accéder à certaines fonctionnalités (téléchargement des mises à jour et/ou ajout/consultation de tickets) selon les sélections effectuées lors de l'ajout de l'utilisateur par le Support logiciel.
Administrateur	Le niveau *Administrateur* autorise l'accès à l'ensemble des options et fonctionnalités de **Guide**. Il permet de consulter la documentation, de télécharger les mises à jour, de créer/consulter des tickets, de contacter le Support logiciel et d'autoriser l'ajout d'utilisateurs.

Seul le Support logiciel de Maestro peut créer des comptes et attribuer des accès.

Limitations en matière de sécurité

Malgré toutes les fonctionnalités mises en place dans **maestro***, la sécurité demeure un aspect où la vigilance s'impose en tout temps. Un fin finaud pourrait évidemment consulter l'information des projets et/ou s'intéresser et accéder aux tables utilisées pour la génération de rapports, de listes et d'analyses D/V et, par déduction ou forage de données, identifier l'hôte de certaines informations statiques.

Table

«... Une table est un ensemble de données organisées sous forme d'un tableau où les colonnes correspondent à des catégories d'information et les lignes à des enregistrements, également appelés entrées. »

Source : https://fr.wikipedia.org/wiki/Table_(base_de_donn%C3%A9es)#:~:text=Dans%20les%20bases%20de%20donn%C3%A9es,des%20enregistrements%2C%20%C3%A9galement%20appel%

C3%A9s%20entr%C3%A9es. le 6 juillet 2020

À RETENIR

- L'administrateur de **maestro*** détient les accès à tous les modules achetés par l'entreprise. C'est cette personne qui est responsable de l'octroi des droits d'accès dans **maestro*** et des configurations liées à la sécurité.
- Les droits d'accès sont attribués sur une base individuelle mais aussi par groupe d'utilisateurs.
- Comme tout bon système, l'accès à **maestro*** est lié à l'utilisation d'un mot de passe; Maestro recommande d'ailleurs de faire usage des meilleures pratiques en ce sens.
- Différents types d'accès peuvent être attribués aux utilisateurs, selon les produits et le type de connexion utilisés.
- Il est possible d'appliquer nombre de restrictions individuelles, liées aux différents modules et options de **maestro***, mais aussi de limiter l'accès aux projets, aux compagnies et aux données des employés.
- Les documents et courriels en provenance de **maestro*** peuvent également faire l'objet d'une sécurité additionnelle.
- Des niveaux d'accès et l'accès aux modules sont déterminés par un groupe d'utilisateurs auquel appartient l'employé.
- Une fonctionnalité de **maestro*** appelée *boucle de sécurité* permet d'attribuer ou non, à certains utilisateurs, le droit de modifier des transactions créées par d'autres utilisateurs.
- Il est possible de grouper des compagnies en domaines afin de dupliquer des droits administrateurs pour ce domaine et d'ainsi créer des administrateurs locaux.

À RETENIR

- La sécurité des compagnies créées peut être *globale* (et identique pour toutes) ou *locale*.
- L'accès au portail **Guide** est également protégé par l'utilisation de mots de passe.

PISTES DE RÉFLEXION POUR LA MISE EN PLACE DE LA GESTION DE LA SÉCURITÉ DANS MAESTRO*

- ☐ Quels sont les groupes d'utilisateurs (utilisateurs ayant des fonctions communes) dans votre entreprise?
- ☐ À quels modules et fonctionnalités doivent avoir accès ces groupes d'utilisateurs, dans **maestro***?
- ☐ Souhaitez-vous que les utilisateurs puissent voir et/ou modifier et/ou ajouter des données dans les options auxquelles ils auront accès?
- ☐ Dans le cas où vous avez plus d'une compagnie, est-ce que la sécurité à appliquer doit être la même pour toutes?
- ☐ Est-ce que des utilisateurs doivent être en mesure d'apporter des modifications à des transactions réalisées par d'autres utilisateurs?

ANNEXE - BONNES PRATIQUES EN MATIÈRE DE GESTION DES MOTS DE PASSE

L'accès à **maestro*** est protégé par l'utilisation d'un mot de passe. Il importe à tous les utilisateurs de choisir celui-ci judicieusement et d'adopter des pratiques sécuritaires. Après tout, ce sont les données de l'entreprise qui sont en jeu!

Voici, à ce sujet, les pratiques recommandées :

1. **Un mot de passe ne doit pas consister en une information connue**

   On ne le dira jamais assez : personne ne doit être en mesure de deviner un mot de passe. Trop souvent encore sont utilisés des suites de nombres, des dates de naissance et des termes tels « bienvenue », « allo », « password », etc. Bref, les termes qui peuvent vous être associés par

plusieurs ou qui ont un sens sémantique simple sont à éviter.

2. **Un mot de passe doit être modifié au moindre soupçon**

Jamais aucune entreprise ou organisation sérieuse ne vous demandera de lui communiquer votre mot de passe par courriel ou par téléphone. Dès le moindre soupçon, il est recommandé de changer son mot de passe sans tarder.

3. **Il est recommandé de modifier régulièrement son mot de passe**

Il est conseillé de modifier ses mots de passe tous trois mois pour tout ce qui relève du travail (codes d'ordinateur, de session, etc.) puisqu'il s'agit généralement de données sensibles.

4. **Un mot de passe doit être fort et complexe**

Une des consignes probablement les plus importantes consiste à utiliser un mot de passe qui n'est pas courant ou facilement détectable par des pirates. Il est essentiel de créer des codes robustes. Pour ce faire, créer des mots de passe :

- avec un minimum de 12 caractères
- composé d'un mélange de lettres majuscules et minuscules
- incluant des caractères spéciaux (exemples : &"#_^) et des chiffres.

Un mot de passe robuste doit se composer de 4 types de caractères différents : majuscules, minuscules, chiffres, et signes de ponctuation ou caractères spéciaux (€, #...).

Éviter également les suites logiques simples comme 123456, azerty, abcdef, etc. qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes. De plus, ne jamais utiliser d'expressions courantes, de titres ou de paroles de chansons, de titres de films ou de citations.

« Pour la septième fois de suite, 123456 trône au sommet de la liste des pires mots de passe de l'année de la firme de sécurité informatique SplashData. »

Radio-Canada, publié le 19 décembre 2019

Quelques méthodes pour créer un mot de passe solide

- La méthode des premières lettres : Un tiens vaut mieux que deux tu l'auras, qui donne *1tvmQ2tl'A;*
- La méthode phonétique : J'ai acheté huit CD pour cent euros cet après-midi, qui

donne *ght8CD%E7am*;

- Le procédé de Schneier : J'aime manger de la pizza tous les jeudis pour souper, qui devient *Jmdlptljps*;
- La méthode consistant à choisir quatre ou cinq mots au hasard, tels bon cheval agrafe batterie;
- La méthode consistant à inclure un mot dans une langue étrangère, soit par exemple bon horse agrafe batterie.

NOTE : Surtout, ne pas utiliser de techniques prévisibles comme le remplacement de « E » par « 3 » ou de « a » par « @ ». De telles techniques donnent un faux sentiment de sécurité et rendent le mot de passe très vulnérable aux attaques par tentative de deviner qui sont automatisées.

5. **Un mot de passe doit être confidentiel; jamais on ne doit le partager!**

Les occasions où l'on peut être tenté de partager son mot de passe sont multiples : un collègue de confiance a oublié le sien, on veut faire vite et sauver du temps, etc. Accepteriez-vous de partager votre NIP aussi facilement?

NIP

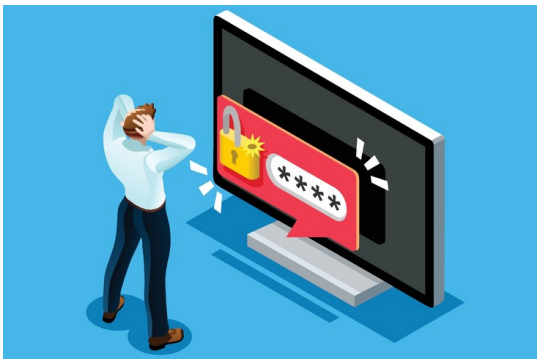
NIP signifie Numéro d'Identification Personnel (PIN en anglais). Le NIP est un code confidentiel composé exclusivement de chiffres permettant d'authentifier le détenteur d'une carte à puce (carte de paiement ou de retrait, par exemple).

6. **Un mot de passe ne doit être utilisé que pour un seul compte et un seul logiciel**

Il est recommandé d'utiliser des mots de passe distincts pour tous les comptes même s'ils sont détenus par une seule et même personne. Les pirates informatiques auront tôt fait d'utiliser votre mot de passe Facebook pour débloquer votre compte Twitter, Instagram, courriel et autres. Toutefois, il est toujours possible d'utiliser une même base et de changer les chiffres et les caractères spéciaux selon les plateformes ou les logiciels. Pour les machines, cela restera tout aussi difficile à casser que des mots de passe totalement différents.

7. **Les mots de passe ne doivent pas être centralisés dans un document, qu'il soit papier ou non**

Qui n'a jamais noté un mot de passe sur un petit bout de papier? Toutefois, tout comportement observé n'est pas nécessairement bon à reproduire. :-) Il existe désormais des gestionnaires de mots de passe qui répondent au besoin tout en étant beaucoup plus sécuritaires.



Gestionnaires de mots de passe

Ces outils, aussi appelés “coffre-forts” de mots de passe, permettent de centraliser ceux-ci de manière sécurisée (les fichiers sont cryptés). On peut accéder à ces fichiers à partir d'un super mot de passe.

Les gestionnaires de mots de passe les plus connus sont KeePass, ZenyPass, et Password Safe. D’autres outils sont également bien notés par les sites spécialisés, comme Dashlane ou encore LastPass.

Il importe toutefois de se souvenir de son super mot de passe et de bien le protéger en évitant les connections Internet mal sécurisées !

8. **Éviter de réutiliser un mot de passe**

Bien qu'il soit tentant de réutiliser d'anciens mots de passe, cette pratique est fortement déconseillée.

Pour en savoir plus sur les pratiques recommandées pour la gestion des mots de passe, consulter :

https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-sur-mots-passe.html

Sources :

https://www.economie.gouv.fr/particuliers/creer-mot-passe-securise

https://start.lesechos.fr/apprendre/universites-ecoles/mots-de-passe-les-7-bonnes-pratiques-a-adopter-1176387

Dernière modification : 24 mai 2024