GUIDE DE MISE EN ŒUVRE DE LA NORME PA-DSS

NORME DE SECURITE DES DONNEES D'APPLICATION DE PAIEMENT HOTELLO

Hotello V6.8.yyy.zzz

- Dernière révision: le 15 Mai, 2019 -
Première version Septembre 2010

TABLE DES MATIÈRES

Chapitre 1 - Introduction

1.1 OBJECTIFS ET PORTÉE

Ce document sert de guide de référence pour les hôteliers/marchands qui utiliseront le logiciel Hotello de MINGUS Software Inc. (MINGUS). La certification PA DSS de Mingus permet à ses clients de simplifier leurs certifications PCI DSS. Ce document porte spécifiquement sur HOTELLO V6.8.yyy.zzz - logiciel de gestion hôtelière.

Ce document présente nos recommandations pour une utilisation conforme de notre logiciel aux normes de l'Appendice A du PA DSS 3.2. Les hôteliers sont cependant les seuls responsables de la mise en œuvre de leur propre environnement de conformité PCI. Le but de ce document est de vous aider à vous conformer aux normes PCI, en apportant suffisamment d'informations pour installer, configurer et exploiter HOTELLO de la bonne façon.

1.2 À PROPOS DU CONSEIL DES NORMES DE SÉCURITÉ PCI

Le Conseil des normes de sécurité du secteur des cartes de paiement est un forum international ouvert, lancé en 2006, qui est responsable du développement, de la gestion, de l'éducation et de la sensibilisation en ce qui concerne les normes de sécurité du secteur des cartes de paiement, notamment : les normes de sécurité des données (Data Security Standard, DSS) applicables aux hôteliers /marchands par exemple, la norme de sécurité des données des applications de paiement (Payment Application Data Security Standard, PA-DSS) et les exigences des dispositifs de saisie du NIP (Pin-Entry Device, PED).

1.3 À PROPOS DES NORMES DE SÉCURITÉ DES DONNÉES PCI (PCI DSS)

Le standard de sécurité PCI DSS est un ensemble d'exigences détaillées permettant aux hôteliers /marchands d'avoir un cadre de conformité afin de fournir une sécurité adéquate des informations de paiement de leurs clients. Ce standard est maintenu à jour par le conseil des normes de sécurité PCI SSC. Plus de 200 membres en comité révisent ces normes régulièrement. Le conseil, a été créé pour simplifier les normes dans l'industrie du paiement. Les membres fondateurs du conseil sont American **Express, Discover Financial Services, JCB International, MasterCard et Visa Inc.**

PCI DSS présente 12 groupes d'exigences incluant la gestion de la sécurité, la politique de sécurité, les procédures, l'architecture réseau, la conception de logiciels et d'autres mesures de protection. Ce guide permet d'aider les entreprises à protéger leurs données et à prévenir les fraudes par l'utilisation d'une application de paiement validée.

Pour de plus amples informations, veuillez consulter le site du conseil des normes de sécurité pour l'industrie des cartes de paiement: "https://pcisecuritystandards.org".

1.4 PUBLIC CIBLE

Ce document est destiné aux personnes suivantes:

- Les clients de MINGUS (Opérateurs d'hôtels)
- Les installateurs/développeurs de MINGUS
- Les vendeurs/revendeurs de MINGUS
- Le service à la clientèle de MINGUS
- Formateur du personnel de MINGUS

Prendre note que Mingus n'utilise pas de revendeurs ou d'intégrateur

1.5 PRÉALABLE

Ce document assume que vous possédez les connaissances ou compétences suivantes:

- Connaissance opérationnelle des ordinateurs
- Connaissance des concepts réseau de base
- Expérience avec les systèmes d'exploitation et les plateformes supportés par HOTELLO
- Bonne connaissance de logiciel HOTELLO
- Être familier avec les périphériques de HOTELLO

1.6 DIFFÉRENCE ENTRE LA CONFORMITÉ PCI ET LA CERTIFICATION PA-DSS

Comme fournisseur de logiciel, nous devons nous respecter les normes de sécurité des données d'application de paiement (PA-DSS) pour l'industrie des cartes de paiement (PCI). Pour ce faire, nous avons réalisé l'évaluation et l'examen de la certification de conformité avec une firme d'évaluation externe pour garantir que la plateforme est conforme aux meilleures pratiques de l'industrie des cartes de paiement

Obtenir la conformité PCI DSS est la responsabilité conjointe de l'hôtelier ou de son hébergeur. Ils doivent travailler ensemble pour se conformer aux normes de sécurité en vigueur.

La certification PA-DSS vise à assurer que l'application de paiement vous permettra d'atteindre et de maintenir la conformité PCI DSS en précisant comment l'application de paiement manipule les comptes des utilisateurs, les mots de passe et les données des titulaires de cartes de crédit.

1.6.1 Les 12 conditions du PCI DSS

Création et gestion d'un réseau et d'un système sécurisés

Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte

Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Protéger les données de titulaire de carte

Condition 3 : Protéger les données de titulaire de carte stockées

Condition 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts

Maintenir un programme de gestion des vulnérabilités

Condition 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes

Condition 6 : Développer et gérer des systèmes et des applications sécurisés

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître

Condition 8 : Identifier et authentifier l'accès aux composants du système

Condition 9 : Restreindre l'accès physique aux données de titulaire de carte

Surveillance et test réguliers des réseaux

Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte

Condition 11 : Tester régulièrement les processus et les systèmes de sécurité

Gestion d'une politique de sécurité des informations

Condition 12 : Maintenir une politique qui traite des informations de sécurité pour l'ensemble du personnel

1.7 DOCUMENTS DE RÉFÉRENCE

- Meilleurs pratiques en sécurité: https://fr.pcisecuritystandards.org/minisite/en/
- Norme de sécurité des données d'application de paiement — PA DSS 3.2
- Norme de sécurité des données — PCI DSS 3.2

Chapitre 2 - Guide de mise en œuvre des meilleures pratiques de sécurité

Bien que MINGUS reconnaisse l'importance de soutenir la sécurité des titulaires de carte de crédit et l'intégrité des données, veuillez noter que certaines exigences des normes de sécurité PCI DSS et PCI-SSC sont de la seule responsabilité des clients. Consulter la liste des responsabilités des clients et les standards associés aux PCI DSS sur le site https://www.pcisecuritystandards.org/.

Nom de l'application	Hotello
Version	6.8.yyy.zzz
Dépendances PA DSS	Tender Retail MCM version 4.x Datacap NetePay version 5.05

Table 1

2.1 ARCHITECTURE RÉSEAU

Conformément aux exigences 9.1 du PA DSS, MINGUS sépare l'environnement de développement et de production de son système de réservation, pour en garantir l'intégrité et la sécurité; Afin de rencontrer la norme PCI DSS, vous devez prendre les actions suivantes :

- **Ne pas stocker les données de titulaire de carte sur un système destiné au public** (le serveur web et le serveur de base de données ne doivent pas être sur le même serveur ou VLAN)
- Utiliser la DMZ pour protéger les données des titulaires de carte, **en séparant internet et le système de stockage des données de titulaires de carte** (installer les serveurs web sur la DMZ et le serveur de base de données sur un segment fiable du réseau)
- Référez-vous à la section 3.6 du présent document, pour **prendre connaissance des composants, services, protocoles et ports requis par Hotello**

La figure ici-bas illustre l'architecture réseau recommandée par MINGUS, pour vous conformer aux normes de sécurité en vigueur (PA-DSS), en procurant une meilleure protection de votre réseau informatique et de l'environnement des données de titulaires de carte.

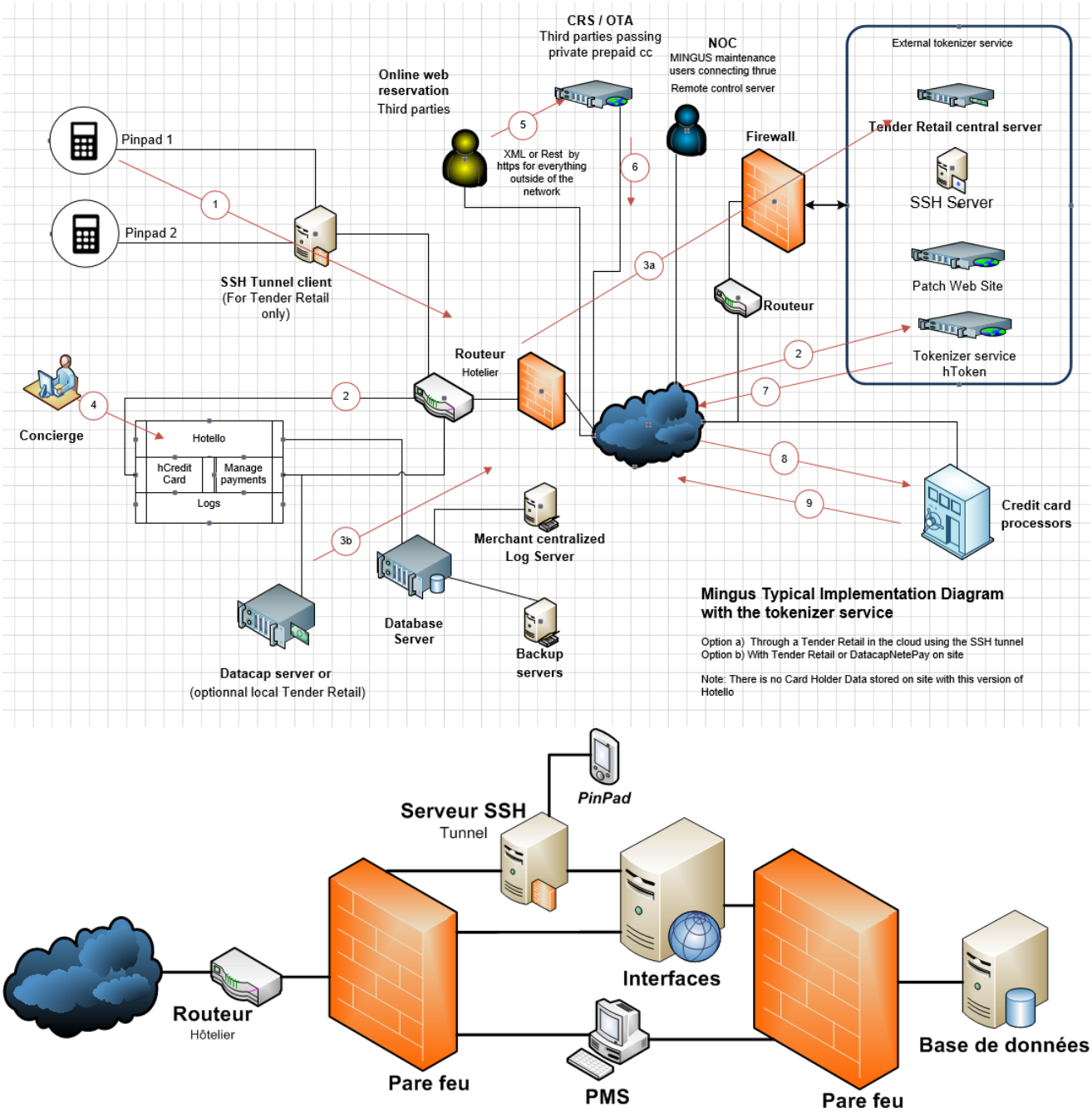


Figure 1 Architecture réseau recommandée par MINGUS Software

Hotello 6.8.yy.zzz élimine le stockage local des données de carte en utilisant un service de jeton. Hotello 6.8.yy.zzz ne stocke que le jeton affilié aux données de la carte d'utilisateur final. Le jeton étant fourni par le fournisseur de services de tokenisation. L'utilisation de cette option aide à réduire le risque de données de carte volée d'une part et à réduire davantage votre coût de certification puisque vous êtes alors admissible à une SAQ simplifié si vous ne stockez pas de données de titulaire de carte localement. De plus, les transactions de commerce électronique sont gérées sur un serveur hDistribution hors site. Chaque Hotello se connectant à l'aide d'un tunnel SSH sur la Bitvise au serveur.

2.1.1 Flux des données de la carte

Comme le présente la figure 1, cette version de Hotello est disponible en 3 options :

a) Avec Tender Retail offert dans le cloud
b) Avec le Tender Retail sur site
c) Avec Datacap sur place

Révisons tout le flux potentiel de données de la carte de crédit :

Le flux d'entrée d'un Pinpad est le numéro 1:

1) Tout d'abord, la transaction de paiement est demandée à Hotello soit à TenderRetail (ou Datacap en fonction de l'installation sélectionnée). Il spécifie à partir de laquelle des Pinpads la transaction doit être acquise
2) Puis TenderRetail (ou Datacap), communique avec le Pinpad approprié et l'active pour recevoir la transaction.
3) TenderRetail (ou Datacap) reçoit les données de la carte, obtient l'autorisation par le numéro de flux 8 et la transmet à Hotello en utilisant le flux 9 via le processus de gestion des paiements de Hotello.
4) Hotello transmet les données de la carte au service de jeton pour obtenir un jeton en utilisant le processus HCreditcard comme indiqué dans le flux 2.
5) Le jeton retourné à l'aide du flux 7 est ensuite conservé dans la base de données Hotello.
6) Le flux 7 pourrait également être utilisé si un employé autorisé doit afficher une PAN en clair. En appuyant sur un bouton dans Hotello, il fait une demande en utilisant HCreditcard au fournisseur de services de tokenisation. Le PAN reçu sera affiché 30 secondes avant d'être de nouveau tronqué par Hotello.

Le flux numéro 4 couvre la façon dont le PAN est manipulé lorsqu'il est entré directement dans Hotello:

7) Lorsqu'un numéro de carte est reçu par téléphone ou autrement, l'utilisateur nommé concierge à la figure 1) l'entre manuellement dans Hotello.
8) Lorsqu'un PAN est capturé par Hotello, il demande automatiquement un jeton à l'aide de HCreditcard par le flux 2, au fournisseur de services de tokenization.
9) Ensuite, si un PAN doit être vu en clair par une partie autorisée, il utilisera le flux 7 comme décrit précédemment.
10) La connexion avec l'acquéreur se fait par l'intermédiaire du gestionnaire de paiement et de la dépendance sélectionnée (Tender Retail opion a ou b ou Datacap)

Le flux 5 couvre la façon dont un PAN est reçu à partir d'un site Web tiers via un serveur central (transaction effectuée sur le serveur central hDistribution):

11) Les données de la carte sont reçues sur un site central dans le serveur hDistribution tel que défini par le tiers comme Expedia, Travelclick ou reservIT.
12) Ensuite, le serveur central hDistribution à l'aide du numéro de flux 2 le remplacer par un jeton.
13) Le jeton est transmis à l'aide du canal SSH à l'Hotello local
14) La connexion avec l'acquéreur se fait par l'intermédiaire du gestionnaire de paiement et de la dépendance sélectionnée (Tender Retail option a ou b ou Datacap)

Le chemin 6 couvre comment un PAN reçu par un tiers via la centrale hDistribution:

15) **Ensuite, le processus du flux 6 est utilisé lorsque le tiers remplacr les données de la carte d'utilisateur final par un jeton temporaire ou un numéro de carte qui ont la même valeur que les données de carte que la carte de l'opérateur.**

2.2 RECOMMANDATION SUR LA CONFIGURATION DES CONNEXIONS SANS FIL

Veuillez noter que **MINGUS interdit formellement l'utilisation des réseaux sans fil (WIFI) avec l'application Hotello** ou **pour transmettre les données des titulaires de cartes de crédit.**

Toutefois, si vous êtes contraint d'utiliser des réseaux sans fil avec l'application Hotello, vous devez vous assurer - conformément à l'exigence 2.1.1 du PCI DSS - que tous les réseaux sans fil par lesquels transitent les données des titulaires de carte crédit ou qui sont connectés à l'environnement des données des titulaires de cartes de crédit, utilisent un chiffrement fort pour l'authentification et la transmission des données.

Pour vous accompagner dans le respect de cette exigence et conformément à l'exigence 6.3 du PA-DSS, MINGUS enjoint tous ses clients de suivre - pour tous les réseaux sans fil qui transportent les données de titulaires de carte ou qui sont connectés à l'environnement des données de titulaires de carte - les recommandations suivantes :

Activer le pare-feu sur le routeur pour contrôler l'accès à internet et prévenir les intrusions
Installer des pares-feux périmétriques entre tous les réseaux sans fil et l'environnement des données des titulaires de cartes, et configurer ces pares-feux pour refuser ou de contrôler (si ce trafic est nécessaire à des fins commerciales) tout le trafic de l'environnement sans fil dans l'environnement de données de titulaire de carte
Vérifiez que le microprogramme sur les appareils sans fil est mis à jour pour supporter un cryptage fort pour l'authentification et la transmission sur les réseaux sans fil
Vérifiez que la valeur par défaut des chaines de communauté du SNMP sur les appareils sans fil a été modifiée
Vérifiez les autres paramètres par défaut du fournisseur sans fil liées à la sécurité ont été modifiées, le cas échéant
Utiliser le protocole WPA2 - parce qu'il possède une clé chiffrement robuste et applique les éléments obligatoires de la norme IEEE 802.11i - en lieu et place des protocoles WEP et WPA-PSK (WPA personnel) qui ne respectent pas les normes de sécurité en vigueur
Assurez-vous que la clé de chiffrement (WPA) du réseau sans fil est changée chaque fois que son intégrité est remise en cause • durant l'installation, • chaque fois que quelqu'un connaissant la clé change de poste ou ne travaille plus pour l'entreprise.
Changer les mots de passe par défaut et utiliser des mots de passe forts pour le routeur • Assurer vous que l'identifiant et le mot de passe par défaut du compte administrateur a été changé, pour éviter les prises de contrôle hostiles.

• Le nouveau mot de passe du compte administrateur du routeur ne doit jamais être exposé
S'assurer de changer le *mot de passe* / la *phrase de passe* des points d'accès
Utiliser les routeurs sécurisés • Automatiser la mise à jour des logiciels et micro logiciels intégrés des routeurs, afin de prévenir ou de corriger d'éventuelles failles de sécurité. • Utiliser la fonction de filtrage des adresses MAC, afin d'établir la liste des équipements informatiques habilités à se connecter au réseau WIFI. • Arrêter le routeur, lorsqu'il n'est pas utilisé pendant une période prolongée comme les vacances d'été.
Ne jamais partager votre réseau privé WIFI • Mettre le routeur dans un emplacement sécurisé, pour prévenir les connexions hostiles par câble réseau. • Réduire la puissance du signal WIFI pour éviter sa propagation hors de la zone ciblée. • Désactiver la diffusion du nom du réseau (SSID), pour éviter qu'une personne non autorisée ne détecte le réseau.
Désactiver les services dangereux comme Bluetooth et UPnP car ils peuvent être utilisés par un Trojan qui a infecté un ordinateur au sein du réseau - pour ouvrir une passerelle vers le routeur connecté à internet et permettre à des connexions provenant de l'extérieur d'infecter l'ordinateur.
Assurer vous êtes protégés contre les attaques par déni de service et les attaques par balayage de port, qui sont fréquemment utilisées par les hackers pour s'introduire dans un réseau
Ne pas activer la fonction DHCP, qui permet d'assigner automatiquement les adresses IP aux postes de travail. MINGUS recommande l'utilisation des adresses IP dédiée.
Désactiver la configuration à distance du routeur.
Surveiller le réseau en activant et en enregistrant les journaux d'événements du routeur.
Conseiller et former le personnel sur un usage plus sûr d'internet, système de messagerie et des équipements WIFI

2.3 ACCÈS À DISTANCE

Conformément à l'exigence 8 du PCI DSS, tous les accès distants provenant d'un réseau public ou extérieur au réseau de l'application de paiement doivent utiliser une authentification à deux facteurs pour rencontrer les exigences de la norme PCI DSS.

Afin de vous aider à vous conformer à cette exigence, MINGUS vous recommande de suivre les règles suivantes :

- Désactiver tous les accès à distance qui ne sont pas munis et d'un chiffrement fort et d'un système d'authentification à deux facteurs; comme un VPN par exemple. Plusieurs vols

ont lieu par L'utilisation sur l'internet de port pas suffisamment sécurisés comme RDP ou FTP;
    - Établir une connexion VPN via un pare-feu avant que l'accès ne soit autorisé.
- Ne jamais installer de matériels ou de logiciels qui ne sont pas requis ou qui interfèrent avec le fonctionnement normal des technologies d'authentification à deux facteurs pour l'accès à distance sécurisé;
- Se méfier des compagnies qui utilisent les connexions à distance pour leur soutien technique, sans que vous acceptiez leurs connections.
- Modifier les paramètres par défaut dans le logiciel d'accès à distance (par exemple, les mots de passe par défaut de changement et d'utiliser des mots de passe uniques pour chaque client).
- Autoriser les connexions uniquement à partir des adresses IP/MAC (connus) spécifiques.
- Utiliser une authentification forte et mots de passe complexes pour les connexions (aux exigences de PA-DSS 3.1.1 par 3.1.11)
- Permettre la transmission de données chiffrées selon PA-DSS exigence 12.1
- Activer le verrouillage de compte, après qu'un certain nombre d'échec de connexion tentatives (répondre aux exigences de PA-DSS 3.1.9-3.1.10)
- Activez la fonction de journalisation.
- Restreindre l'accès à des environnements client au personnel autorisé.

Conformément à l'exigence 10.1 du PA-DSS, MINGUS utilise « ConnectWise » pour permettre à son équipe de maintenance et de soutien d'assister par le biais d'une connexion à distance à deux facteurs.

Plus d'informations sur le produit ConnectWise peut être trouvé :

https://docs.connectwise.com/ConnectWise_Control_Documentation/On-premises/Advanced_setup/Payment_Card_Industry_Compliance_(PCI)

Notez également que l'accès à distance ne doit être activé que si nécessaire, et immédiatement désactivé après utilisation. L'ordinateur Hotello doit se verrouiller automatiquement et une nouvelle connexion exigera que le mot de passe local ouvre l'accès de telle sorte qu'un accès ne puisse être autorisé que par le client.

2.4 AUTHENTIFICATION SÉCURISÉE

Pour se conformer à la condition 8 du PCI DSS et restreindre l'accès aux composants (application, systèmes d'exploitation, les serveurs, les bases de données, etc.) liés à l'application de paiement des ou aux données des titulaires de cartes de crédit, MINGUS recommande à ses clients de suivre les directives suivantes :

- Changer/désactiver les *identifiants, mots de passe et autres paramètres par défaut définis par les fournisseurs* durant l'installation et/ou la configuration.
- S'assurer que chaque utilisateur a un identifiant et un mot de passe uniques et différents
    - *L'identifiant DOIT ÊTRE DIFFÉRENT du mot de passe*;
- S'assurer que le mot de passe de chaque utilisateur ait au moins la complexité suivante :
    - une longueur minimale d'au moins 7 caractères

- Comporte à la fois des *caractères numériques* et des caractères *alphabétiques (majuscules et minuscules)* et optionnellement mais recommandé des *caractères spéciaux* comme : ?, !, *, etc.
- *Différent des 4 derniers mots de passe*;

- S'assurer que la *période de conservation des mots de passe* soit inférieure à 90 jours;
- S'assurer que *le composant requiert une saisie du mot de passe pour les sessions d'utilisateur inactives pendant plus de 15 min*;
- S'assurer que *le composant verrouille les comptes d'utilisateur après plus de six tentatives de connexion infructueuses*;
- Supprimer/désactiver les comptes d'utilisateur inactifs au moins tous les 90 jours.
- Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société.

Le module d'accès est conçu pour appliquer ces règles.

2.5 TRAITEMENT PARTICULIER DES DONNÉES SENSIBLES

Pour se conformer à l'exigence 1.1.5 du PA-DSS, MINGUS recommande de suivre ces règles quand durant la manipulation des données d'identification sensibles (données de bande magnétique, codes de validation de carte, NIP ou NIP de blocage) :

- Les données d'identification sensibles sont uniquement collectées lorsque cela est nécessaire pour résoudre un problème particulier.
- Ces données sont stockées à un emplacement spécifique connu dont l'accès est restreint.
- Une quantité minimale de données d'identification sensibles est collectée, selon la quantité nécessaire pour résoudre un problème spécifique.
- Ces données sont supprimées de façon sécurisée immédiatement après leur utilisation, y compris: Fichiers journaux; Fichiers de débogage; Autres sources de données reçues des clients.

Pour des besoins de maintenance, Hotello génère des logs qui ne contiennent qu'une empreinte des informations de carte de crédit. Un exemple est disponible dans l'Appendice A de ce document.

2.6 GESTION SÉMANTIQUE DES VERSIONS

Chaque version de l'application Hotello est définie par le numéro suivant : W.X.Y.Z (*6.8.yyy.zzz*), ou chaque élément fait référence à une modification de l'application HOTELLO

- **W** correspond aux changements qui ont un impact sur la sécurité et/ou sur les conditions de la norme PA-DSS : Améliorations majeures de l'application de paiement
- **X** correspond aux **changements majeurs qui n'ont aucun impact sur la sécurité ou les conditions de la norme PA-DSS** (mise à jour du serveur de base de données, nouveau module) ou aux **changements mineurs qui ont un impact sur la sécurité et/ou sur les conditions de la norme PA-DSS (**Migration vers le protocole $\mathrm{TLS}_{1.2+}$ pour se prémunir de la vulnérabilité logicielle : PODDLE présent dans le protocole $\mathrm{SSL}_{3.0}$**)**

- Y et Z correspondent aux **changements mineurs qui n'ont aucun impact sur la sécurité ou les conditions de la norme PA-DSS**
  - **Y** : Corrections qui affectent la base de données et nouvelles fonctionnalités
  - **Z** : Corrections qui n'affectent pas la base de données

2.7 SÉCURITÉ DES SYSTÈMES DE MESSAGERIE

Pour se conformer à l'exigence 11.2 du PA-DSS, MINGUS déconseille à ses clients d'accepter ou de transmettre des données de titulaire de carte de carte de crédit par courriel.

Cependant, si vous êtes contraint d'utiliser un système de messagerie pour transmettre ou recevoir des données de titulaire de carte de crédit, vous devez suivre les règles suivantes :

- Ne pas utiliser un système de messagerie publique (comme Gmail, Yahoo, Hotmail, etc.) pour recevoir ou transmettre les informations de cartes de crédit. Sauf si vous paramétrez la conformité du contenu : https://support.google.com/a/answer/1346934
- Utiliser des protocoles de messagerie sécurités (tels que PGP) qui rendra les informations de carte de crédit inutilisables durant leur transport.

Chapitre 3 - Guide de mise en œuvre de la sécurité — Norme de sécurité des données d'application de paiement

3.1 LES DONNÉES DES TITULAIRES DE CARTES DE CRÉDIT

3.1.1 Sauvegarde des données des titulaires de cartes de crédit

Avant tout, veuillez noter que *depuis la version 6.8.yyy.zzz* - conformément à l'exigence 1.1.5 du PA-DSS- Hotello ne sauvegarde plus les données d'identification sensibles : la totalité des données de la bande magnétique, le code de validation (CAV2, CID, CVC2, CVV2), le numéro d'identification personnelle (NIP).

Par ailleurs, conformément aux exigences 1.1 et 2.3 du PA-DSS, Hotello 6.8.yyy.zzz utilise un *système de Tokenisation* pour sauvegarder le PAN (numéro de compte primaire) de la carte de crédit; Seules les données de titulaires de carte suivantes:

- *L'empreinte du PAN (seuls les quatre premiers et derniers chiffres du PAN sont affichés en clair)*
- *Le nom du titulaire de la carte de crédit*
- *La date d'expiration (EXP) de la carte de crédit*

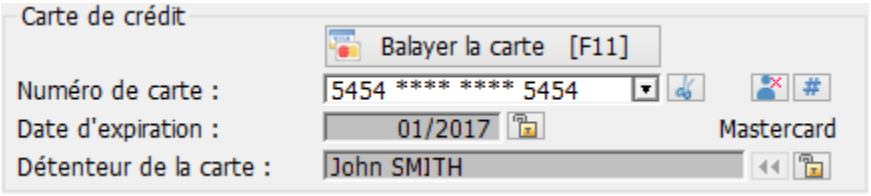
sont sauvegardées par Hotello sur le disque, dans la base de données, les rapports ou les logs pour que les informations de cartes de crédit ne puissent être utilisées qu'aux seules fins d'identification.

Hotello appelle automatiquement le système de tokenisation après avoir reçu les données du titulaire de la carte dans le système. L'utilisateur ne peut pas désactiver la tokenisation et le PAN est toujours rendu illisible par le système de tokenisation.

Pour de plus amples informations concernant les rapports et logs sauvegardés sur le disque, veuillez consulter l'annexe A du présent document.

3.1.2 Affichage des données des titulaires de cartes de crédit

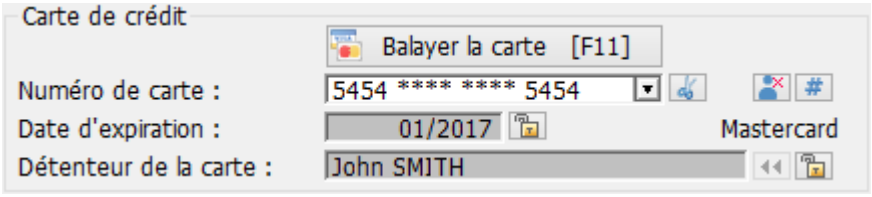
Pour se conformer à l'exigence 2.2 du PA-DSS, Hotello masque le PAN excepté les quatre premiers et derniers chiffres - aux seules fins d'identification - durant le traitement (création, modification ou l'annulation) des réservations et la facturation.



Il est toutefois important de souligner que, pour satisfaire à l'exigence 3.3 du PCI DSS, HOTELLO permet aux usagers - disposant des droits requis - d'afficher en clair le PAN d'une carte de crédit donnée. Il est toutefois important de souligner que seul le personnel ayant un besoin professionnel légitime doit être autorisé à consulter la totalité du PAN. Le PAN est alors affiché durant 30 secondes, par la suite il est ensuite tronqué, durant ces 30 secondes le PAN est disponible dans la mémoire du poste Hotello

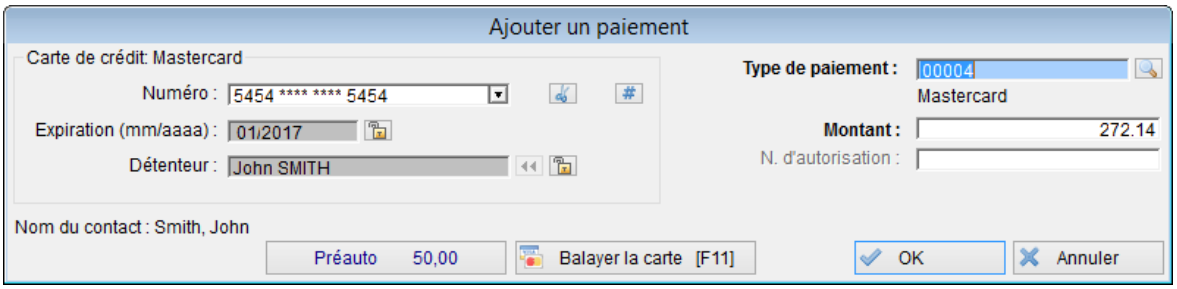
Comment d'afficher en clair/masquer le PAN d'une carte de crédit donnée ?

- **À partir de l'écran de réservation**



  - Le bouton # permet d'afficher en clair le PAN
    Hotello communique avec le système de Tokenisation pour récupérer le PAN correspondant au Token lié à la réservation
  - Le bouton #× pour masquer le PAN

- **À partir de l'écran de paiement**



- Le bouton  permet d'afficher en clair le PAN

  Hotello communique avec le système de Tokenisation pour récupérer le PAN correspondant au Token lié à la réservation, noter que le PAN ne s'affiche que 30 secondes.

- Le bouton  pour masquer le PAN

Cependant, il est important de spécifier, que seul le personnel ayant un besoin professionnel légitime doit être autorisé à afficher l'ensemble du PAN, l'administrateur doit configurer le niveau de sécurité pour donner un accès spécifique à ceux-ci. Veuillez consulter l'article 3.2.2 de ce document qui explique comment définir la permission pour les différents rôles d'utilisateur

3.1.3 Conservation des données des cartes de crédit

Pour supprimer données d'identification sensibles de cartes de crédit stockées par les versions précédentes de l'application de paiement conformément à l'exigence 1.1.4 du PA-DSS, Hotello utilise une procédure automatique à deux étapes - qui insère des informations aléatoires dans la base de données à chacune des étapes et un « Sweep» https://firebirdsql.org/manual/gfix-housekeeping.html (automatique) de la base de données pour ***Supprimer les données d'identification sensibles de cartes de crédit*** (*données de bande magnétique, codes de validation de carte, NIP ou NIP de blocage*).

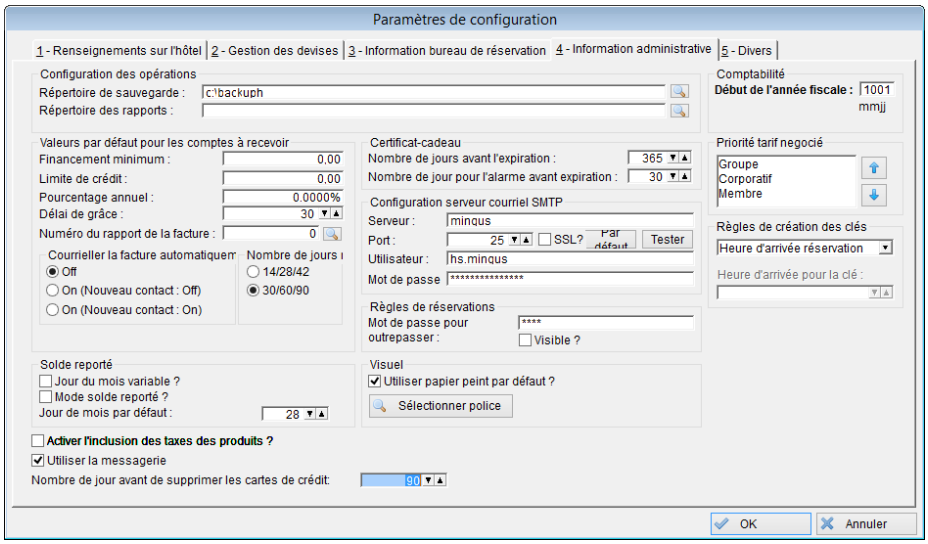
Pour se conformer à l'exigence 2.1 du PA-DSS et permettre à ses clients de rencontrer l'exigence 3.1 du PCI DSS qui préconise de limiter la quantité de données sensibles stockées et d'en restreindre les délais de conservation aux obligations professionnelles, légales et réglementaires, Hotello permet de ***Supprimer* du système de Tokenisation *les cryptogrammes (PAN) ayant dépassé leur période de conservation.***

MINGUS recommande d'utiliser ***Active@Kill Disk - Hard Drive Eraser*** - Ou tous logiciels basés sur l'algorithme de Guttmann, qui permet d'imprimer un certificat confirmant le nettoyage du disque - pour effacer les disques *avant l'installation* ou *après la désinstallation* de l'application Hotello.

Comment définir la période conservation des informations de carte de crédit dans le système de Tokenisation?

Pour rencontrer l'exigence 3.2 du PCI DSS, MINGUS recommande à ses clients de définir une période de conservation - *qui doit être la plus courte possible* - des données des titulaires de carte de crédit.

1. À partir du menu principal de HOTELLO, sélectionner l'option [Configurer]
2. Sélectionner l'onglet [Généralités]
3. Cliquer le bouton [Renseignements sur l'hôtel]
4. Sélectionner l'onglet [Information administrative] et ouvrir la fenêtre suivante



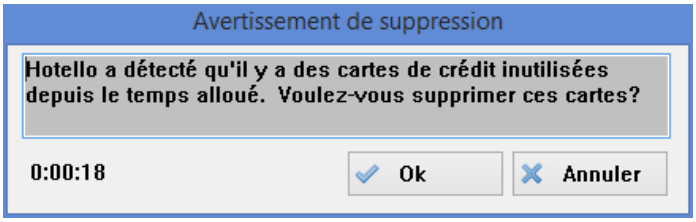
5. Saisir la période de conservation désirée dans le champ « Nombre de jours avant de supprimer les cartes de crédit »
6. Cliquer le bouton [OK] pour sauvegarder les changements

Comment demander au système de Tokenisation de supprimer les cryptogrammes ayant dépassé leur période de conservation ?

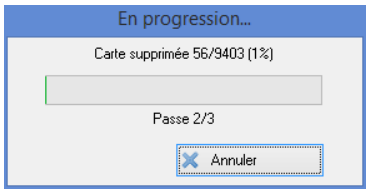
Hotello **exécute automatiquement** - sans intervention humaine - cette opération chaque jour. Pour connaitre tous les endroits où l'application de paiement stocke les informations de cartes de crédit, veuillez-vous référer à *l'annexe A du présent document*

À chaque audition de nuit, HOTELLO vérifie s'il y a des cartes crédit qui ont dépassées leur période de conservation, ***dans la base de données***

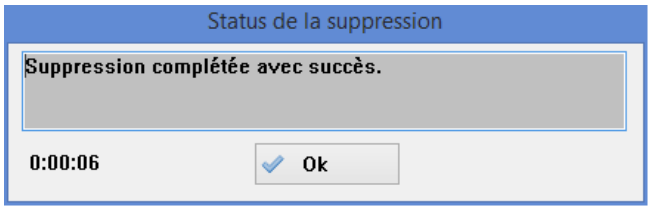
1. S'il y a au moins une carte de crédit ***répondant aux critères ci-dessous***, HOTELLO démarre le processus de suppression en ouvrant la fenêtre ici-bas
   - La période de conservation (*date d'audition – date de la dernière utilisation*) de la carte de crédit *est supérieure* à la période de conservation configurée
   - La carte de crédit *n'est liée à aucune* pré-autorisation ouverte (sans capture)
   - La carte de crédit *n'est liée à aucune* réservation ouverte (in-house, réservé, liste d'attente, …)



2. Cliquer [OK] pour confirmer le démarrage du processus de suppression des cartes de crédit
3. HOTELLO débute la suppression des cartes de crédit en ouvrant la fenêtre suivante (pour permettre aux usagers de suivre l'évolution du processus)



4. À la fin du processus, HOTELLO ouvre la fenêtre suivante



Configuration logicielle sous-jacente : Il n'y a pas d'autres exigences à l'égard du logiciel sous-jacent, si ce n'est l'exigence générale de la section 3.4 ici, car Hotello ne stocke pas de CHD ou de SAD.

3.1.4 Transmission des données des titulaires de cartes de crédit

Afin de protéger les informations sensibles transitant via internet et conformément à l'exigence 11 du PA-DSS, MINGUS utilise :

- Les solutions de paiement intégrées : ***Datacap*** ou ***Tender Retail*** pour *se connecter aux plateformes de paiement*;
- ***Un système de tunnels SSH*** authentifié par un certificat AES-256 pour protéger les communications entre :
  - *Hotello* et *hDistribution* : centrale de réservation permettant de communiquer avec les CRS partenaires (telles hFastbooking, hAvailPro ou hGuestFolio);
  - *Hotello* et *les solutions de paiement* : Datacap ou Tender Retail
  - *HOTELLO et son portail de réservation en ligne*
- ***HTTPS*** (***Apache*** avec ***un certificat*** $\boldsymbol{TLS}_{1.2+}$) pour protéger les *communications entre Hotello et les systèmes suivants : système de Tokenisation, Passerelles de paiements, Gestionnaire de licences, Système de réservations en ligne.*

3.1.5 Gestion des clés

Il n'y a aucune clé impliquée dans Hotello car la version Hotello 6.8.yyy.zzz ne stocke aucune donnée de carte. Il y a l'API HCreditcard utilisé pour se connecter avec le service de jetons, le Tender Retail ou Datacap, mais ceux-ci ne sont pas réglables et sont des fonctions automatisées.

Pour effacer les données de cryptage historiques pour la version précédente, l'outil d'effaçage décrit dans la section 3.1.3 sera utilisé. Les clés cryptographiques sont rendues irrécupérables chaque fois que les clés ne sont plus utilisées conformément aux exigences de gestion des clés dans PCI DSS.

3.2 LES DROITS D'ACCÈS

Pour accéder à Hotello, tout utilisateur qui pourrait voir ou affecter la sécurité du système doit avoir un nom d'utilisateur unique et un mot de passe fort et dans certaines situations un jeton d'authentification à plusieurs niveaux. Cette situation doit être maintenue même après les modifications apportées au système ou lorsqu'ils changent leurs informations d'identification. Aucun utilisateur par défaut n'est autorisé. En outre, Hotello n'accepte pas de nombreux niveaux ou rôles pour ses utilisateurs. Il est

important, lors de la création d'un utilisateur que vous assignez le moins de privilège d'accès aux données confidentielles nécessaires pour le faire fonctionner. Normalement, vous devriez avoir 3 niveaux d'utilisateurs lorsque vous regardez les données confidentielles:

- Utilisateurs qui n'ont pas besoin de voir les données de titulaire de carte (encore besoin d'un identifiant d'utilisateur unique et mot de passe)
- Utilisateurs qui ont besoin de l'utiliser (avec le moins de privilège)
- Administrateurs système qui administrent les privilèges dans Hotello

Vous devez également désactiver les utilisateurs inutilisés ou par défaut.

3.2.1 Sécurité des identifiants et des mots de passe

Pour se conformer à l'exigence 3.3 du PA-DSS, HOTELLO sale le mot de passe et utilise SHA256 pour le hachage.

Par ailleurs HOTELLO utilise le service hMingusKey pour valider le mot de passe de l'équipe de support et de maintenance. Conformément à la condition 3 du PA-DSS, le service hMingusKey génère – sans intervention humaine - chaque jour un mot de passe aléatoire qui respecte les normes de sécurité en vigueur.

Mingus n'utilise aucun revendeur ou intégrateur et le personnel de Mingus est tenu d'utiliser des ID uniques et l'authentification sécurisée conforme de PCI-DSS pour accéder à tous les PC, serveurs et serveurs de bases de données dans l'environnement client.

3.2.2 Gestion des droits d'accès

Conformément aux exigences 3.2 du PA-DSS et aux règles édictées dans la *section 2.4 du présent document*; Hotello permet de gérer les accès des employés en se basant sur leur besoin professionnel, grâce aux fonctionnalités suivantes :

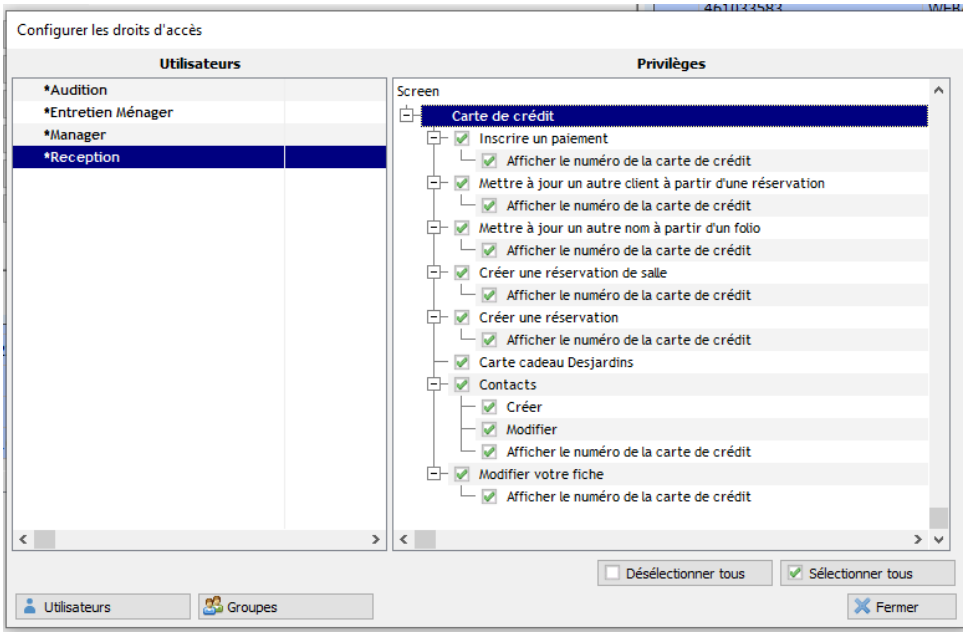
- ***Gérer les droits d'accès des employés***
- ***Désactiver les comptes des utilisateurs ayant dépassé le nombre de tentatives de connexion maximum*** (6)

  Les comptes des utilisateurs verrouillés, ne peuvent être déverrouillés que par des usagers disposant des droits requis
- ***Pour chaque utilisateur qui a accès à des données sensibles, essayer d'accéder à des données sensibles après 15 minutes d'inactivité va l'enregistrer automatiquement.***

Pour de plus amples informations, veuillez consulter les normes de sécurité édictées par le Conseil des normes de sécurité PCI à l'adresse suivante : «https://pcisecuritystandards.org»

Comment gérer les droits d'accès des employés ?

1. À partir du menu principal de HOTELLO, sélectionner l'option [Configurer]
2. Sélectionner l'onglet [Généralités]
3. Cliquer le bouton [Droits d'accès]

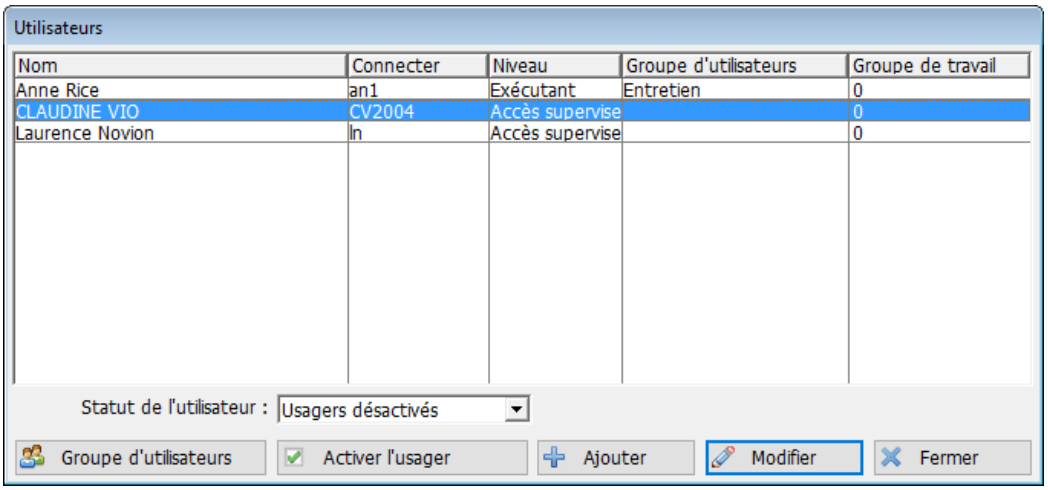


Décocher "Afficher le numéro de la Carte de Crédit" va désactiver la possibilité de voir le numéro complet de la carte de crédit.

Conformément à l'exigence 7 du PCI DSS, MINGUS recommande; fortement; à ses clients de restreindre l'accès aux données des titulaires de cartes de crédit et aux fonctionnalités qui sont liées à l'application de paiement (Afficher en clair le PAN des cartes de crédit, Configurer la durée de conservation des données des titulaires de cartes de crédit, Changer les clés cryptographiques ayant atteint la fin de leur crypto période, ...)

Comment réactiver les comptes utilisateurs ?

1. À partir du menu principal de HOTELLO, sélectionner l'option [Configurer]
2. Sélectionner l'onglet [Généralités]
3. Cliquer le bouton [Configuration des utilisateurs]



4. Utiliser le filtre « Statut de l'utilisateur », pour afficher les utilisateurs inactif
5. Sélectionner l'utilisateur dont on veut réactiver le compte
6. Cliquer le bouton [Activer l'usager] pour activer l'utilisateur

3.3 AUTOMATISER ET CENTRALISER LES LOGS

Conformément aux exigences PA-DSS, Hotello fournit une piste de vérification des activités du système. Pour effectuer cette tâche Hotello a des journaux d'évènements (logs) automatisés et non modifiables qui fournissent la surveillance des accès à Hotello ainsi que les changements affectant le système. Ces journaux sont en lecture seule et ne peuvent pas être supprimés ou écrasés. Hotello suit également d'autres événements qui peuvent montrer une activité frauduleuse. L'enregistrement de chaque événement a deux objectifs :

1. Permettre de voir qui tente d'accéder au système de manière non autorisée.
2. En cas de compromission du système, déterminer où et comment le système a été compromis.

Les événements enregistrés sont les suivants.

- Les journaux d'événements utilisateur (ajout, modification, dernière date de changement de mot de passe, changement de niveau de sécurité)
- L'ouverture du journal d'évènement est également enregistrée dans ce journal système.
- Tous les utilisateurs qui se connectent (y compris les administrateurs et le personnel de maintenance de Mingus)
- Tentatives infructueuses de connexion d'utilisateurs.
- Déconnexion des utilisateurs.
- L'accès aux pistes d'audit des applications est enregistré
- Modification des paramètres de configuration. (Modifications qui affectent la configuration de la carte de crédit; passerelle de paiement ou Pinpad)
- Ajout ou désactivation des utilisateurs (les utilisateurs ne peuvent être retirés d'Hotello, ils sont désactivés)
- Démasquer une carte de crédit, masquer une carte de crédit
- Activation/désactivation du journal de transaction pour débugger la gestion des cartes de crédits (seulement accessible par le personnel autorisé de Mingus)
- Effacer les cartes de crédit, manuellement ou automatiquement via le calendrier programmé.

Les informations suivantes sont enregistrées.

- Date et heure.
- Console. Le nom de l'ordinateur à partir de laquelle l'événement a eu lieu.
- Utilisateur. L'identifiant utilisateur, prénom et nom de famille créant l'événement.
- Description. Le type d'évènement.
- Fichier et numéro d'enregistrement. Dans le cas qu'un évènement affecte un enregistrement.
- Numéro du journal des événements. Un numéro qui aidera à détecter si un enregistrement a été supprimé par un acte externe.
- Type d'évènement.
- Texte. Une description complète de l'événement.

Pour accéder au journal, vous suivez:

Menu principal de HOTELLO -> Administration -> Fonction des interfaces -> Log des accès

Les enregistrements de journaux contiennent beaucoup d'informations, de sorte que vous pouvez utiliser des filtres pour afficher des informations spécifiques que vous recherchez comme indiqué dans le bas de la figure "Parcourir les journaux".

Les journaux ne devraient pas et ne peuvent pas être désactivés et cela entraînera une non-conformité avec PCI DSS.

Les évènements sont également ajoutés au journal des évènements Windows.

Bien que Hotello ne permet pas aux usagers de désactiver la journalisation des activités des usagers dans la base de données, veuillez noter que toute personne ayant un niveau d'accès suffisant sur les serveurs liés à l'application de paiement peut contrevenir à la conformité des exigences 4.1 et 4.4 du PA-DSS. Il est donc de la responsabilité des hôteliers de surveiller tous les accès aux ressources réseau et toutes les activités des utilisateurs sur les composants liés à l'application de paiement.

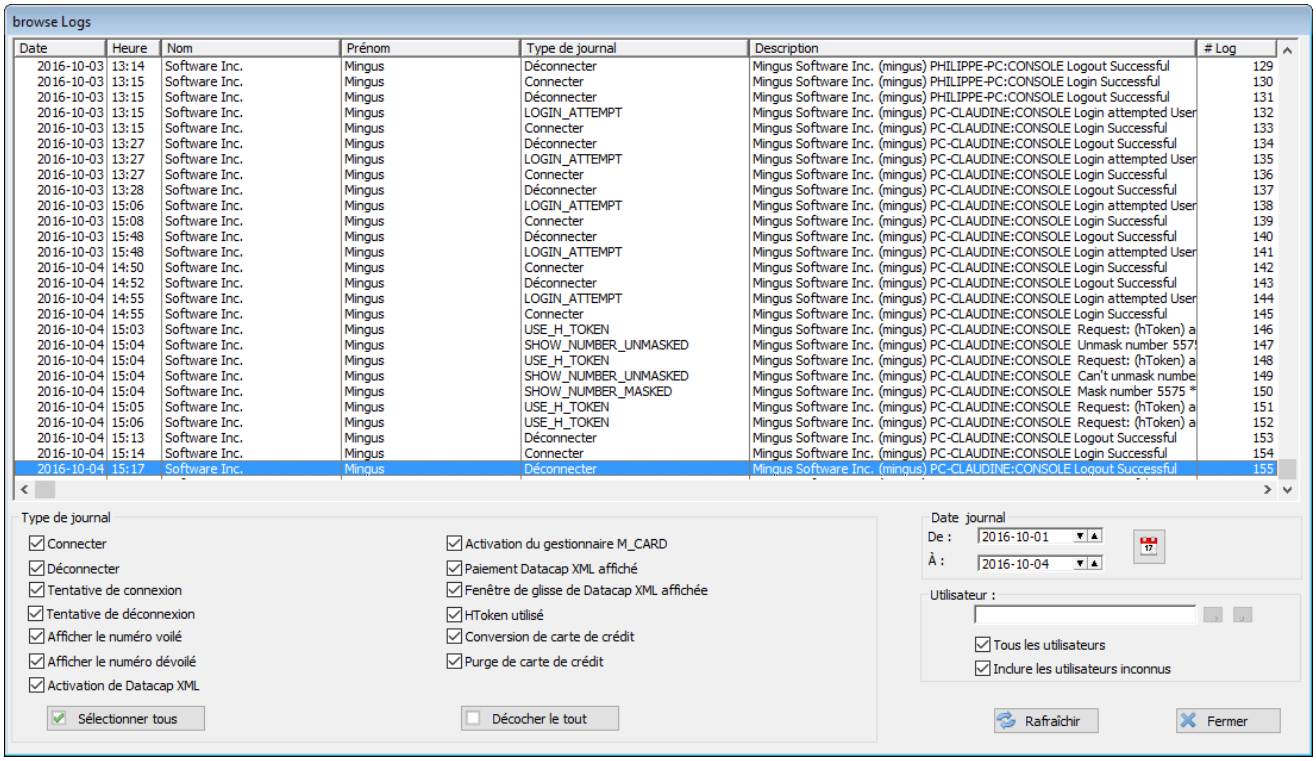


Figure « Browse Logs »

3.4 UTILISATION DES SERVICES, PROTOCOLES, DAEMONS, COMPOSANTS, ET MATÉRIEL ET LOGICIEL DÉPENDANTS

Conformément à la condition 8.2 du PA-DSS, MINGUS recommande d'utiliser ***uniquement*** les services, protocoles, daemons, composants, et matériel et logiciel dépendants, ***nécessaires et sécurisés***, y compris ceux fournis par des tiers, pour toute fonctionnalité de l'application de paiement

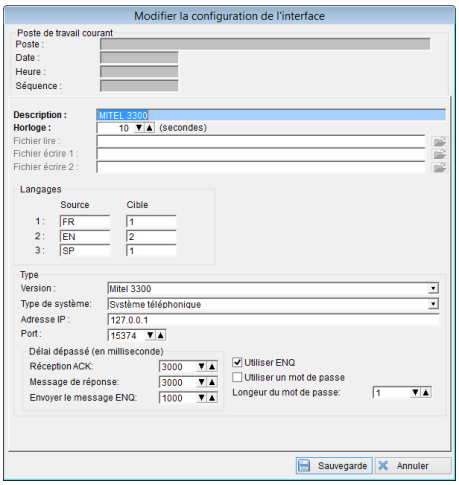
Conformément à cette exigence, veuillez noter que HOTELLO - incluant son application de paiement - nécessite l'utilisation des composantes et ports suivants :

a. **Services**
   - NETePay : Permet de communiquer avec GLOBAL Payments,
   - MCM (merchant connect multi): permet de communiquer avec Tender Retail,
   - Système de Tokenisation : Permet d'externaliser la sauvegarde du PAN des cartes de crédit,
   - hMingusKey : Permet de valider le mot de passe de l'équipe de support et maintenance,
   - hTrWindowsService : pont entre Hotello et MCM et d'autres systèmes de paiements par Service WEB Sécurisé.

b. **Daemons**
   - (DSIClient.ocx) Datacap : Utilisé uniquement durant les opérations avec Datacap et leurs passerelles de paiements, permet de valider et de transmettre les données.

c. **Protocole**
   - HTTPS [internet]: Permet de communiquer avec les passerelles de paiements de manière sécurisée, hTrWindowsService, hMingusKey, MCM et d'autres services WEB.

d. **Ports sortant**
   - 4000, 4041 et 6041 pour la communication exclusive avec Tender Retail pour éviter les attaques DDOS
   - 5350-5355 : Permet de communiquer avec le gestionnaire des licences des produits de MINGUS
   - 3050 : Permet au client Firebird de communiquer avec le serveur Firebird.
   - 443 et 8443 : Permet à MINGUS d'assister les clients par l'entremise de « ConnectWise », d'utiliser le service de tokenisation et à d'autres sites sécurisés
   - 52350-52380 : Permet de se connecter au service hTrWindowsService
   - 250 : Tunnel SSH
   - 212 : Tunnel SSH pour l'utilisation des API de manière sécurisée
   - Les ports permettant de communiquer avec les interfaces sont configurables à partir de HOTELLO
     - *Menu principal de HOTELLO -> Outils -> Interfaces* (interface téléphonique)



Afin de garantir le respect des normes de sécurité en vigueur, MINGUS se réserve le droit ***d'installer un tunnel SSH - authentifié par un certificat - pour protéger les communications*** *des interfaces*

Veuillez noter que ***la responsabilité de la protection des ports alloués à l'application HOTELLO (****configurer le pare-feu afin d'ouvrir uniquement les ports requis****) incombe à l'hôtelier***

e. Composantes

- .NET Framework 4
- EASendMail : composante SMTP 7.3+

f. Logiciels dépendants

- Firebird (ODBC & DBMS): Outil de gestion des bases de données
- FlameRobin, IBExpert & WinSQL: outil d'administration des bases de données
- List & Label : Outil de gestion des rapports
- Bitvise SSH Client : outil qui permet de créer un Tunnel SSH 7.15+

g. Matériels

- Serveur Base de données
- Serveur applicatif
- Poste client
- Poste d'interfaces
- Imprimantes : pour imprimer les rapports, les coupons et les reçus de paiement
- Matériels de connectivité (cartes réseau, routeur) : pour garantir l'accès haute vitesse pour la mise à jour, le dépannage et la formation
- PIN pad comme requis par différents acquéreurs de paiement
- Batterie de secours UPS avec contrôle d'alimentation automatique

3.5 MISE À JOUR DE L'APPLICATION DE PAIEMENT

Pour mettre à jour ses clients - dans le respect des normes de sécurité en vigueur-, MINGUS utilise ce qui suit pour mettre à jour l'application Hotello

- « ConnectWise Control » - via son équipe de support et de maintenance - pour se connecter à l'environnement de production des clients
- Son extranet (http://www.mingussoft.com/download/) pour télécharger les fichiers d'installation et les correctifs de HOTELLO.

Bien que l'approbation du client soit requise pour effectuer la mise à jour, il est important de souligner que MINGUS est responsable de la sécurité de l'environnement du client durant le déploiement de l'application.

Mingus avise tous les clients lorsqu'une mise à jour est disponible via ses différentes plates-formes (email, téléphone), les clients peuvent alors soit télécharger et installer ses mises à jour ou planifier une réunion de support technique Mingus.

Notez que les applications Hotello ont le code signé avec un certificat de code valide pour justifier l'intégrité de l'application, même lorsqu'elles sont mises à niveau. N'installez aucune application sans ce certificat.

3.6 COMMUNICATION AVEC DES PROGRAMMES NON-MINGUS

L'application HOTELLO est destinée à interfacer avec des produits qui ne sont pas développés ou contrôlés par MINGUS (Produits Non-MINGUS). Ces produits Non-MINGUS peuvent être conformes ou non conformes aux Standards de Sécurité du PA-DSS. Conscient de cette problématique, MINGUS recommande fortement à tous les marchands qui connecteront HOTELLO (particulièrement l'application de paiement) à un produit Non-MINGUS ; de s'assurer que ce dernier respecte toutes les exigences du PA-DSS.

3.7 FORMATION DU PERSONNEL

Conformément à la condition 14 du PA-DSS, MINGUS met à la disposition de son personnel, tout l'équipement nécessaire à l'accomplissement de leurs tâches dans le respect total des normes de sécurité en vigueur; et s'assure que ce matériel est mis à jour chaque fois qu'une nouvelle version de l'application de paiement ou de la norme PA-DSS est publiée.

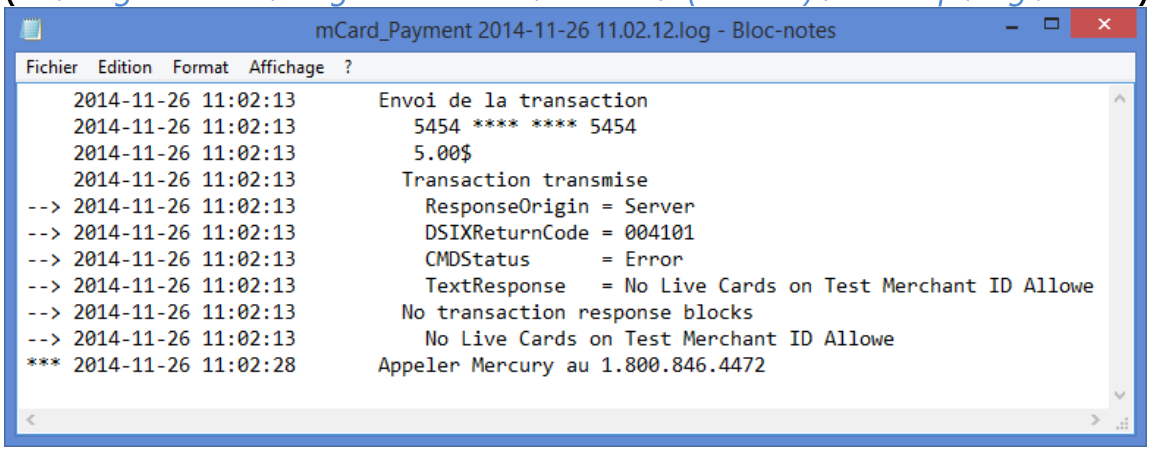
3.8 MISE À JOUR DE CE DOCUMENT

Conscient de l'évolution constante de son application de paiement et de la norme PA-DSS, MINGUS met à jour le « Guide de mise en œuvre de la norme PA-DSS » après chaque changement (majeur ou mineur) de l'application de paiement ou de la norme PA-DSS; et effectue - chaque année - une révision complète du présent document.

Annexe A : Liste des emplacements ou Hotello sauvegarde les informations de cartes de crédit

La base de données de Hotello (*Bien que le choix de l'emplacement de la base de données soit fait par le client, il doit respecter les normes de sécurité en vigueur (confer la section 2.1 du présent document)*)

Le fichier : « *mCard_Payment_YYYYMMDD_HHMMSS.log* » est sauvegardé sur le disque quand le système de paiement rencontre une erreur durant le processus de paiement (*C:\ProgramData\Mingus Software\Hotello\x (# hôtel)\DataCap\Log\MCard*)



Rapport de contrôle des résidents par chambre (*Hotello permet au client de sauvegarde ce fichier ou il le désire sur le disque ou de l'envoyer par e-mail*)

Chambres : Tous
Type de chambre : Tous
Groupe de chambre : Tous
Type de garantie : Tous
Date de la vérification : 10/07/2014

Contrôle des résidents par chambre
Chez Claudine

Page :1

Date de début : 10/07/2014
Date de fin : 10/07/2014

Le total dû inclut les frais du jour qui ne sont pas encore facturés.

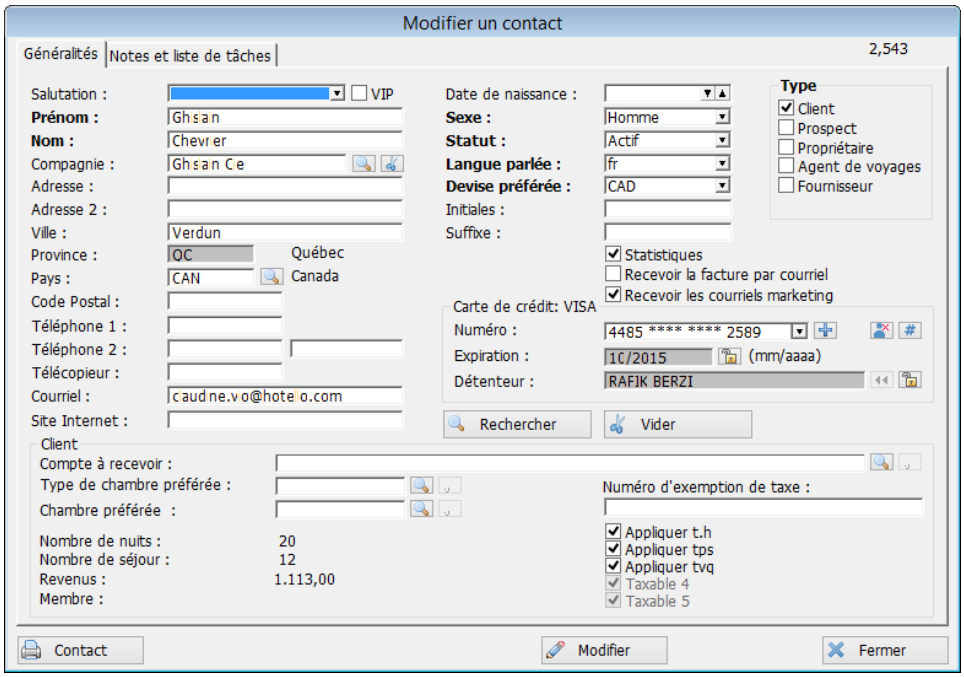
# Conf. / Folio	Chambre / Type de chambre	Nom / Compagnie	Groupe / Compte à recevoir	Garantie / N° Carte de crédit	Arrivée / Départ	A+|A-|En / Nuitée	Code de tarif / Prix à charger	Adresse / Forfait	Frais à la carte	Total des frais du jour	Total dû	Dépassement? / Autorisé pour?
Notes												
Forfait	Description				Numéro	A+|A-|En	Du	Au	Sous folio			
1108-1	123	Chevrier , Ghislain		16H	10/07/2014	1|0|0	NORMAL					**130,27**
127869(A)	REGF	Ghislain Cie		4485**********2589	13/07/2014	1	**130,27**	0,00	0,00	**130,27**	130,27	0,00
1105-1	126	Victorin , Marie		16H	10/07/2014	1|0|0	WEB	4000 St Ambroise				**130,27**
127866(A)	REGF			5454**********5454	11/07/2014	1	130,27	0,00	0,00	**130,27**	130,27	0,00
test amex												
1110-1	134	Daoust , Catherine		16H	10/07/2014	1|0|0	NORMAL	4034 st ambroise				**130,27**
127871(A)	REGNF			4012**********1881	14/07/2014	1	**130,27**	0,00	0,00	**130,27**	130,27	0,00
1111-1	249	Benchemsi , Francoise		16H	10/07/2014	1|0|0	NORMAL	12 Rue Des Écoles				**367,12**
127872(A)	KINGNF	Club Med		5105**********5100	13/07/2014	1	**367,12**	0,00	0,00	**367,12**	367,12	0,00
	Total	**Chambres 4** :				**A+: 4**	**A-: 0**	**EN: 0**				

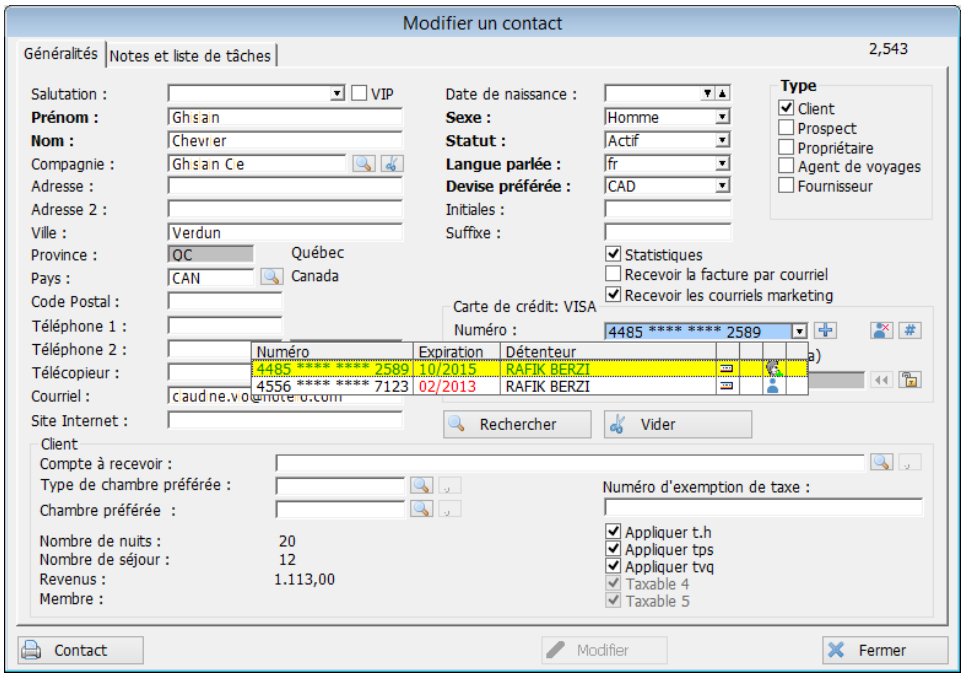
Inclure le type de réservation : ? Réservé : N Résident : O Parti : N Liste des attentes : N Annulé : N Tentatif : N

Imprimé : 11/11/2014 09:39:04, Par : Mingus Software Inc.

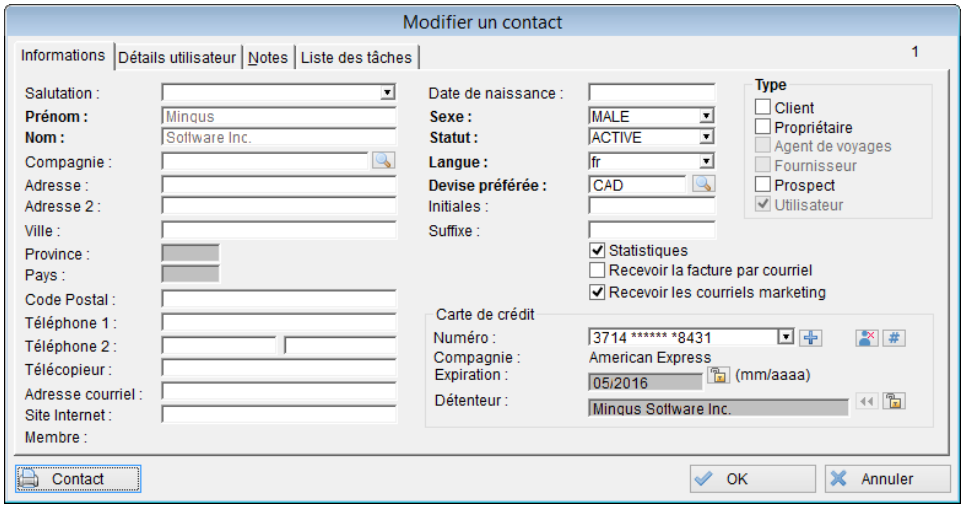
Annexe B : Liste des interfaces qui affichent des informations de cartes de crédit

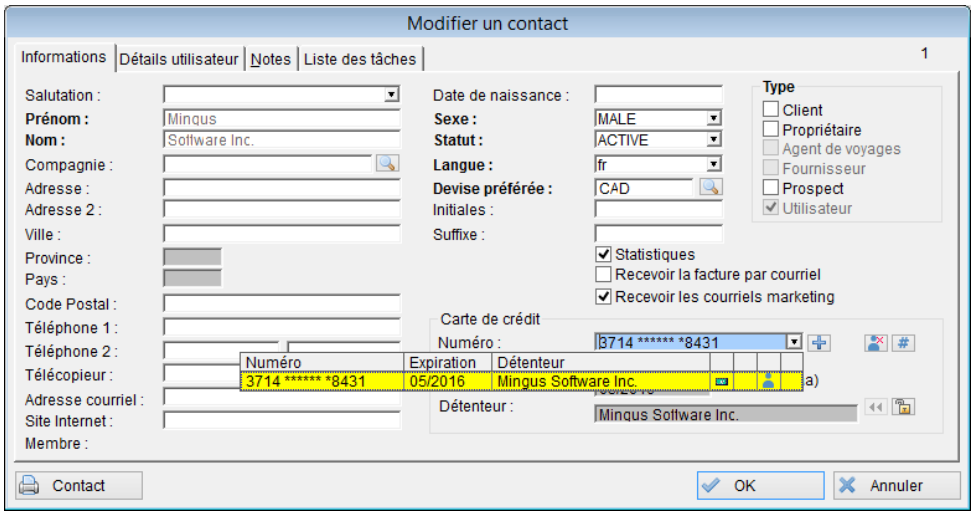
Formulaire permettant de modifier les informations d'un contact (client, prospect, propriétaire, agent de voyage, fournisseur)



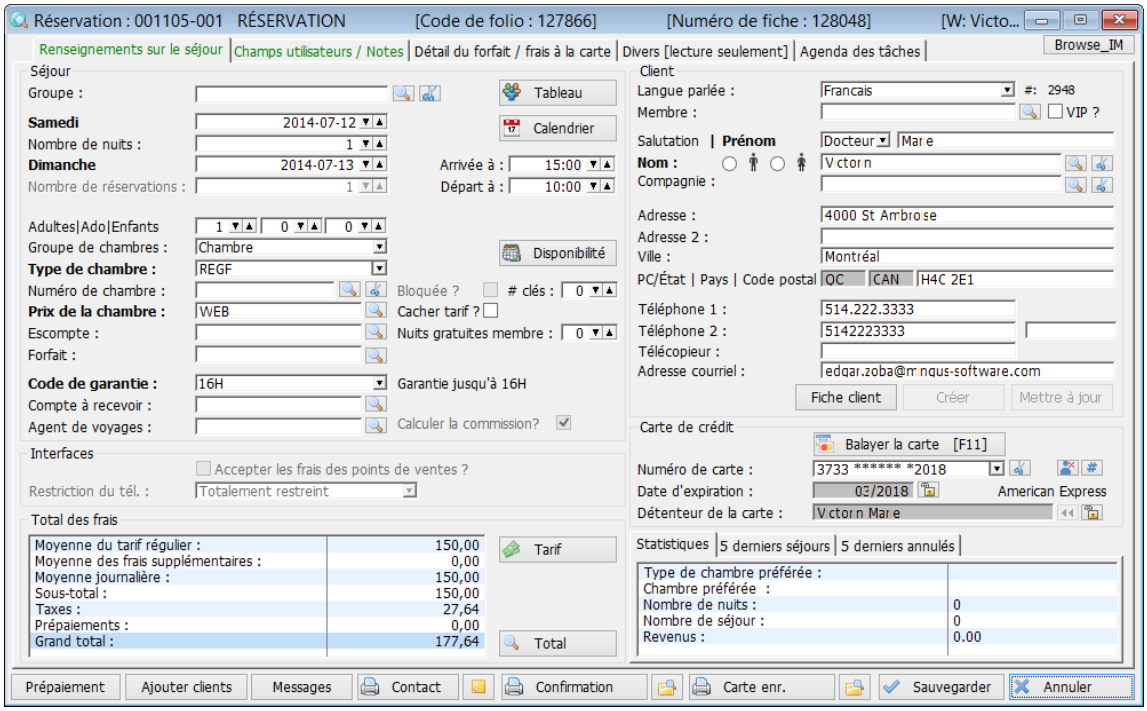


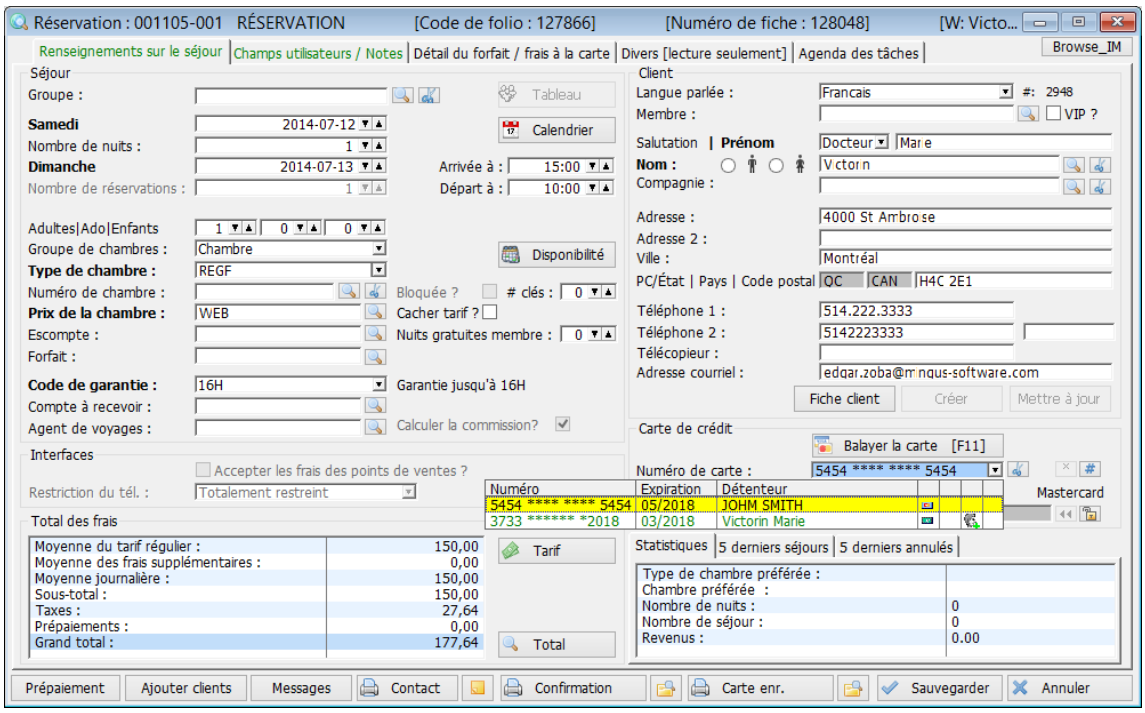
Formulaire permettant de modifier les informations d'un utilisateur



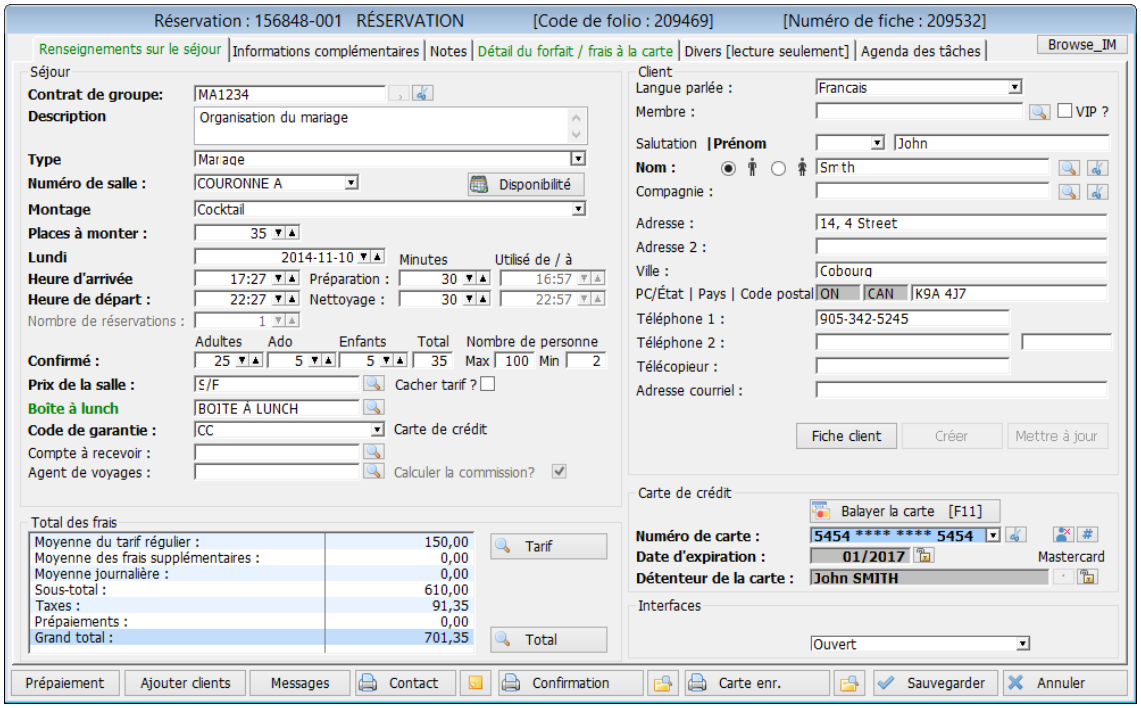


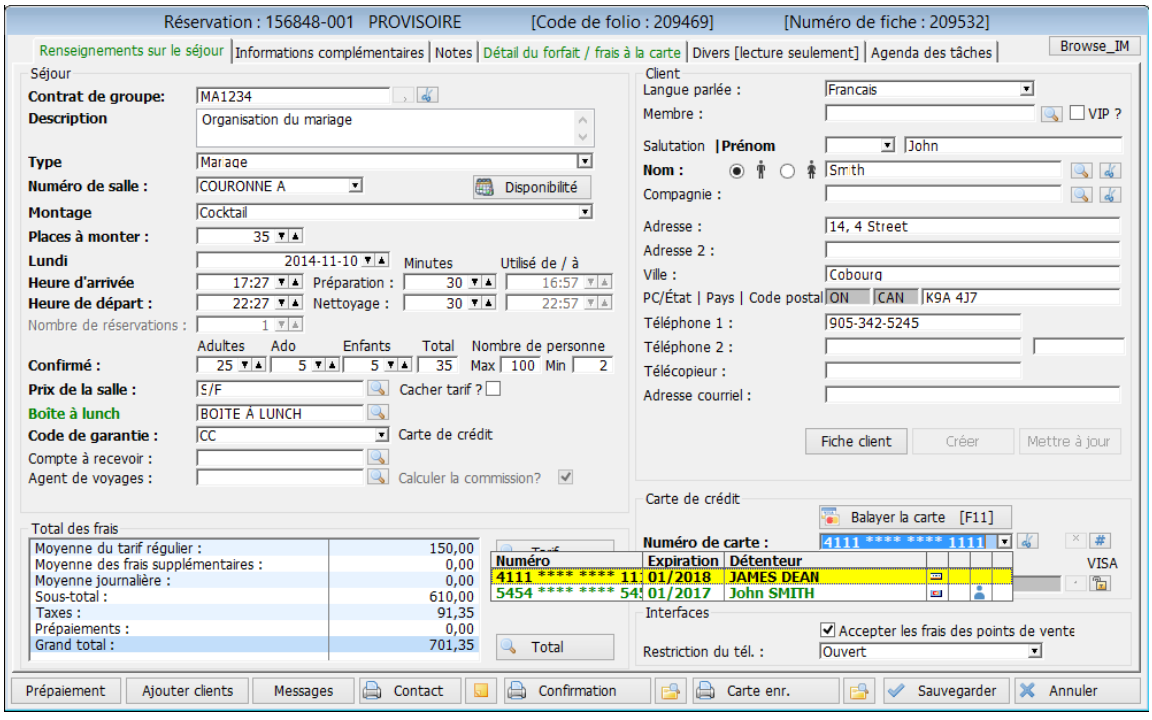
Formulaire de réservation



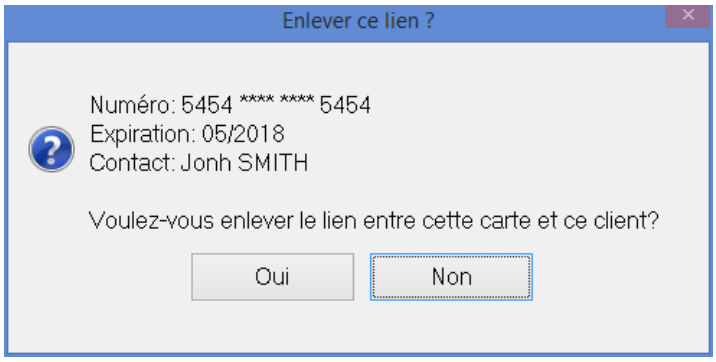


Formulaire de réservation de salle

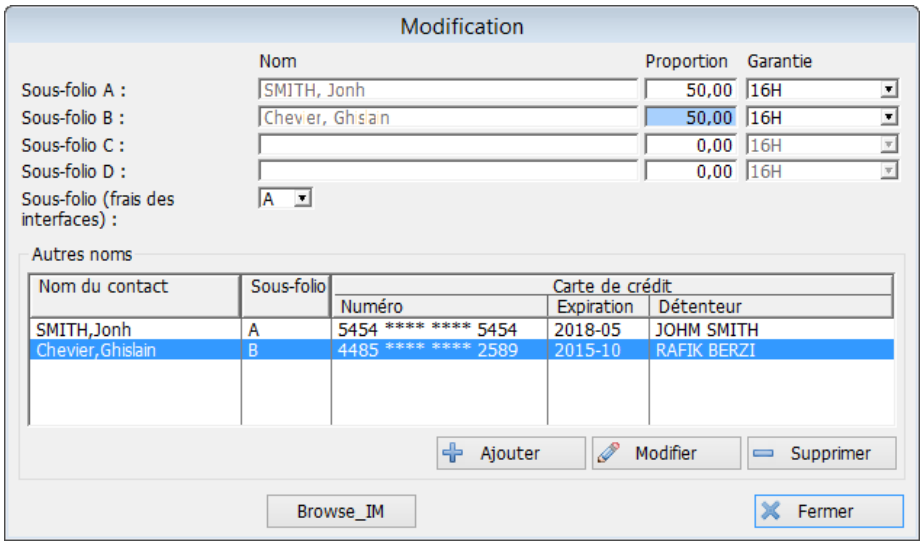




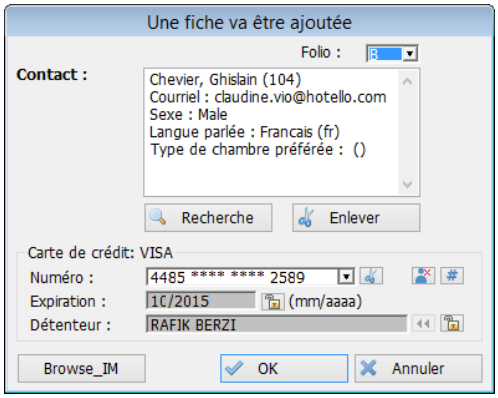
Message qui s'affiche quand on change la carte de crédit d'un client ( ) dans le formulaire de réservation



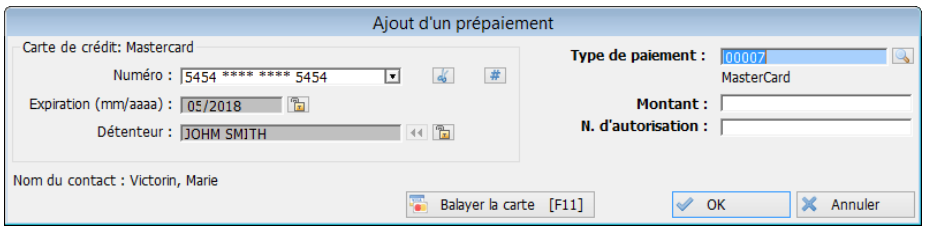
Liste des contacts liée à une réservation

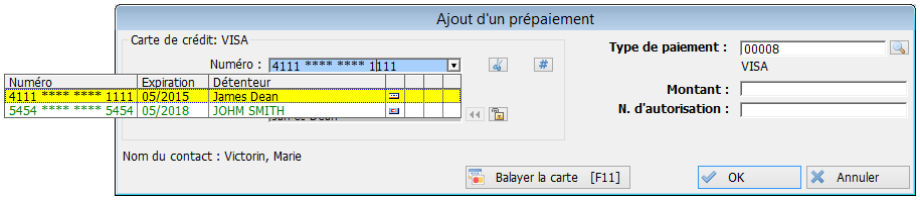


Formulaire permettant d'ajouter un client à une réservation

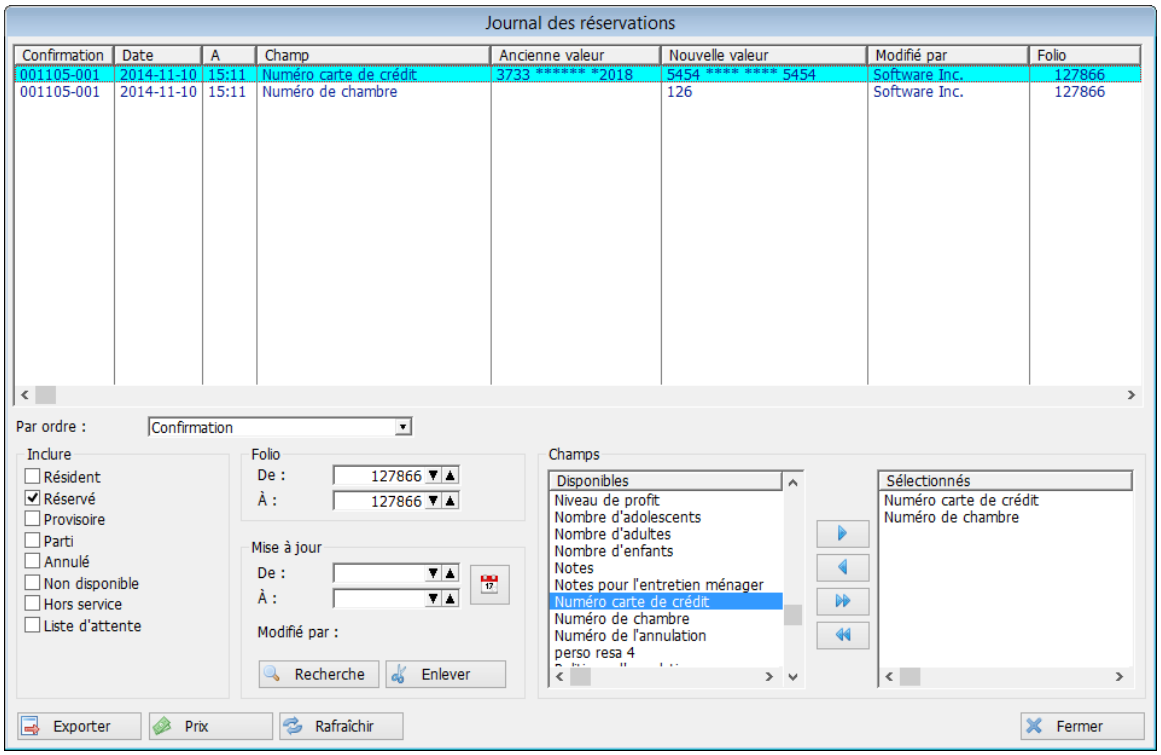


Formulaire permettant d'ajouter un prépaiement

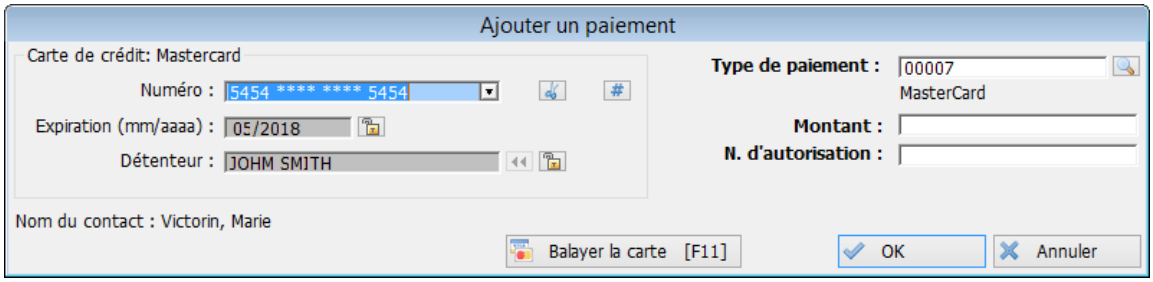


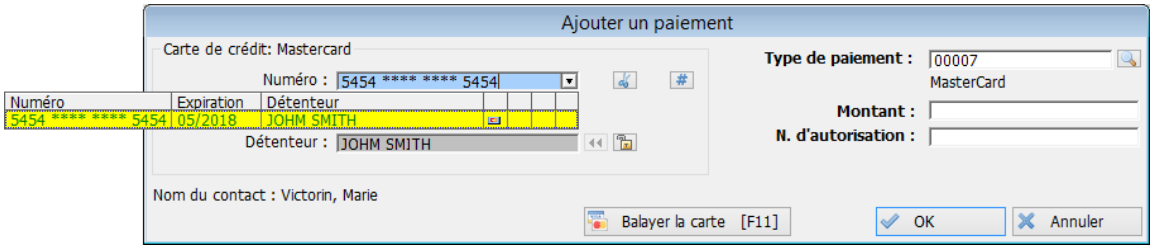


Formulaire permettant d'afficher l'historique d'une réservation

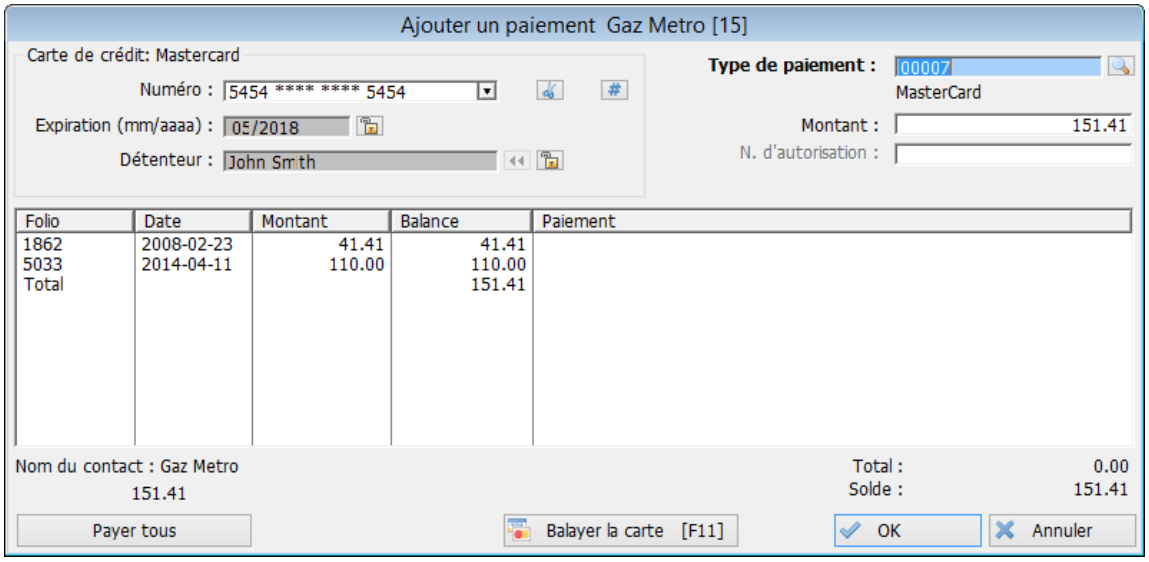


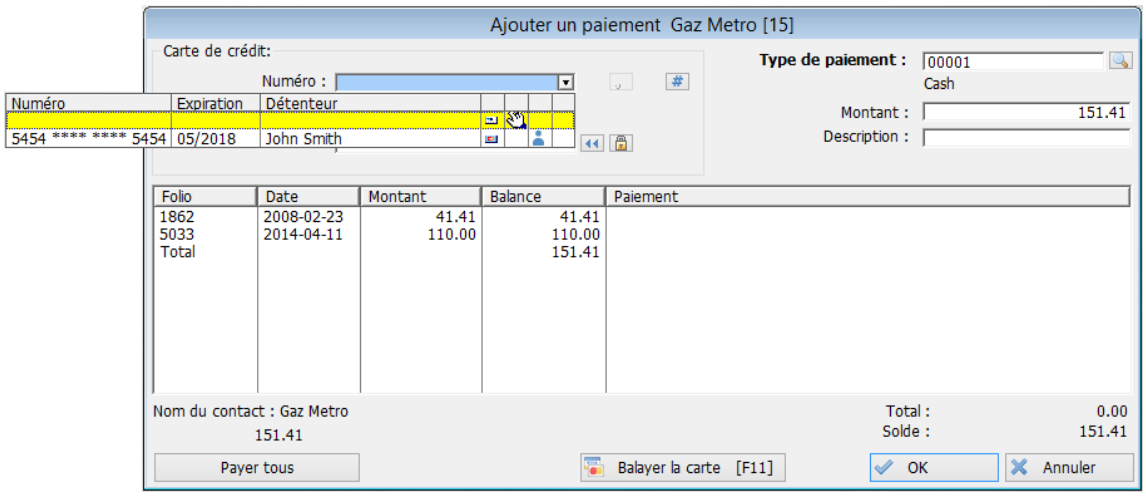
Formulaire permettant d'inscrire un paiement à partir du folio



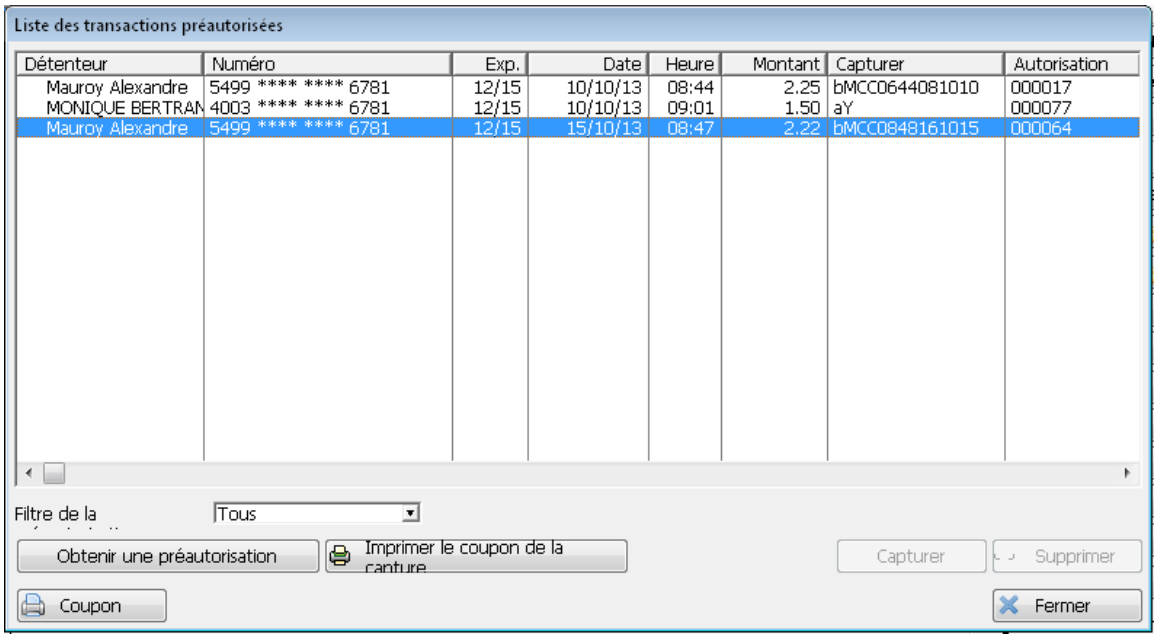


Formulaire permettant d'inscrire un paiement d'un compte à recevoir

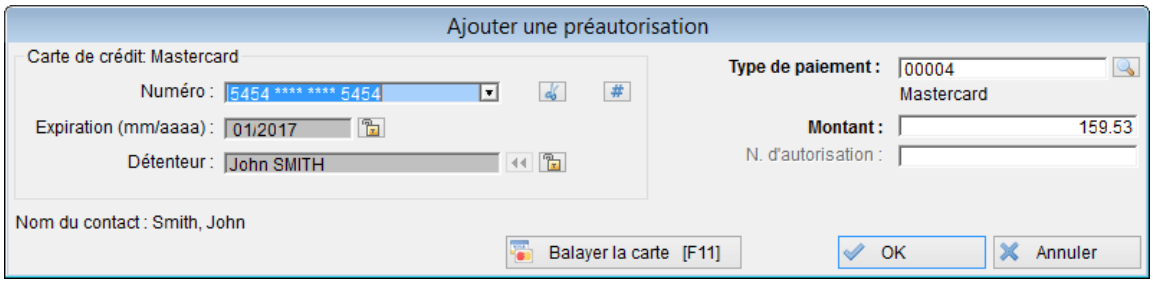


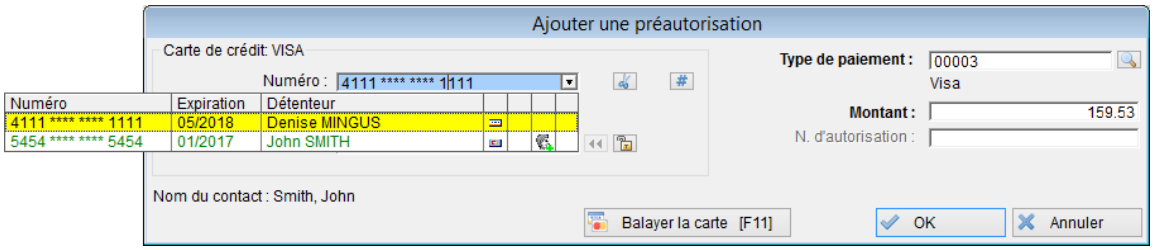


Liste des préautorisations

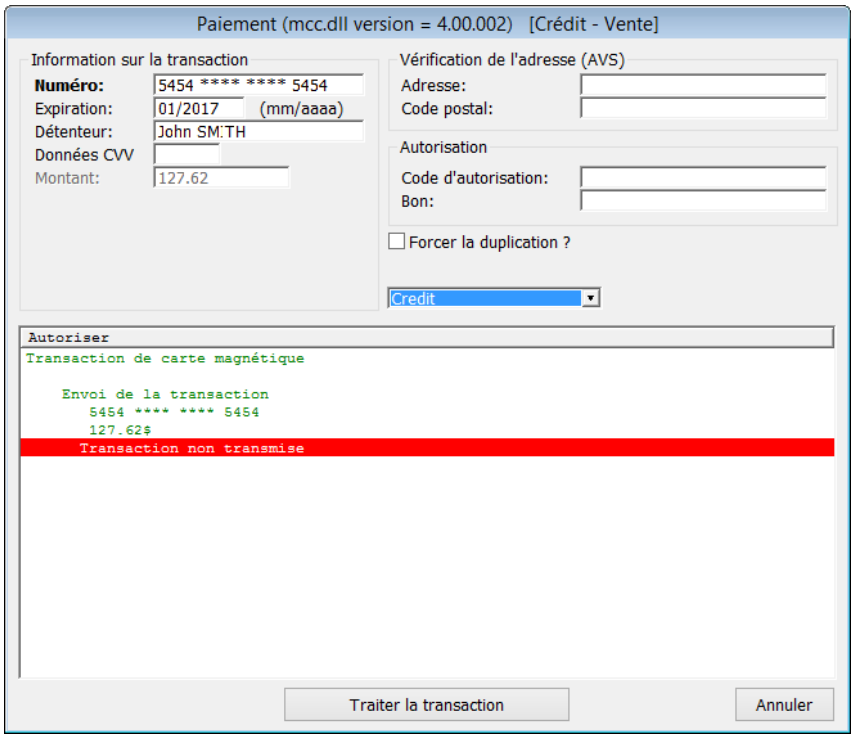


Formulaire permettant d'obtenir une préautorisation





Interface permettant d'effectuer un paiement, une préautorisation, une annulation de paiement ou une capture de préautorisation (avec une carte de crédit)



Annexe C: Détails des révisions

Employé	Mise à jour	Sommaire
Edgar ZOBA	Sep 2010	Mettre à jour le document pour rencontrer les exigences du PA-DSS v2.0
Edgar ZOBA	Jan 2015	- Ajouter le service Hotello Cloud - Mettre à jour le document pour rencontrer les exigences du PA-DSS v3.0
Edgar ZOBA	Avr 2015	Changements requis par PA-DSS 3.0
Edgar ZOBA	Mai 2015	Changements requis par PA-DSS 3.0
Edgar ZOBA	Sep 2015	Changements requis par PA-DSS 3.1
Edgar ZOBA	Fév 2016	Utiliser un système de Tokenisation pour externaliser la gestion du PAN
Edgar ZOBA	Oct 2016	Ajouter la fenêtre de gestion des Logs
Rafik BERZI	Oct 2016	Révision requis par PA-DSS 3.2
Rafik Berzi	Février 2018	Description de la V6.8.yyy.zzz qui est la version utilisant la tokenisation éliminant ainsi le stockage de CHD sur le site du client de Mingus
Rafik Berzi	Mai 2018	Amélioration de la section journal
Rafik Berzi	Mai 2019	Révision générale – Corrections mineures