User Manager

ingenico
ePayments

Table des matières

1. Introduction

Plusieurs fonctions/profils (rôles) différents cohabiteront généralement au sein d'une même société. Un comptable par exemple ne réalisera pas les mêmes opérations qu'un encodeur de paiement ou un intégrateur technique. Logiquement, vous ne souhaitez octroyer que les droits d'accès nécessaires à chaque personne utilisatrice de votre compte et, en outre, assurer le suivi des opérations réalisées par les divers collaborateurs.

L'option User Manager (Gestion des utilisateurs) vous permet d'assigner un profil spécifique à chaque utilisateur afin de lui conférer les droits d'accès dont il a besoin pour exécuter sa mission. Le User Manager est un service supplémentaire disponible pour tous les produits.

Le User Manager vous permet :

- De configurer plusieurs utilisateurs sous un même compte
- De gérer le profil et les droits d'accès de chaque utilisateur
- D'éviter les erreurs critiques des encodeurs de paiement
- D'assurer le suivi des actions menées par chaque utilisateur (nombre de transactions par jour, par exemple)
- De n'autoriser les utilisateurs qu'à consulter leurs propres transactions
- De gérer aisément les droits d'accès au personnel temporaire.

Vous pouvez accéder au User Manager dans le menu de votre compte Ingenico ePayments via “Configuration" > "Utilisateurs” .

2. Activation

Par défaut, votre compte Ingenico ePayments est livré avec deux utilisateurs; le PSPID qui est votre utilisateur par défaut (admin), et un utilisateur supplémentaire.

Si vous avez besoin de plus d'utilisateurs, en fonction de votre abonnement, vous pouvez activer l'option dans votre compte Ingenico ePayments :

1. Allez à "Configuration > Abonnement > Vos options".
2. Rechercher dans la liste des options pour "User Manager up to x users" ("x" définit le nombre d'utilisateurs que vous souhaitez créer: 5, 10, 20 ... 200).
3. Cliquez sur le bouton "Activer".

Selon les options que vous avez activé, vous pouvez créer d'autres utilisateurs avec différents profils et configurations.

3. Profil d'utilisateur

Les principaux profils d’utilisateur supportés par le User Manager sont les suivants :

- consulteur
- encodeur
- super-encodeur
- super-encodeur sans remboursement
- admin sans user management
- admin
- helpdesk admin

3.1 Admin

Un profil Admin dispose de tous les droits d’accès.

Lors de chaque création d’un compte, un utilisateur par défaut est automatiquement généré (le UserID de cet utilisateur par défaut est identique au PSPID). Cet utilisateur par défaut dispose du profil Admin. Il vous est bien évidemment aussi loisible de créer d’autres utilisateurs Admin.

Un utilisateur Admin est le seul utilisateur disposant des autorisations nécessaires à la modification de la configuration du compte.

3.2 Admin sans user management

Le profil Admin sans user management dispose des mêmes droits d’accès que l’Admin, sans cependant avoir accès à l’option User Manager (Gestion utilisateurs).

3.3 Encodeur

Un Encodeur peut soumettre un nouveau paiement via le lien “Nouvelle transaction” dans le menu du compte ou via DirectLink.

3.4 Fraud analyst

Un Fraud analyst peut modifier les listes noires/blanches, consulter la notation des transactions et contester des transactions.

Remarque: Pour que ce profil utilisateur fonctionne correctement, vous devez cocher "Fraud detection" dans les droits d’accès de l’utilisateur.

3.5 Fraud manager

Un Fraud manager peut modifier toutes les pages de configuration appropriées du module de détection des fraudes, modifier les listes noires/blanches, examiner et contester des transactions, etc.

Remarque : Pour que ce profil utilisateur fonctionne correctement, vous devez cocher "Fraud detection" dans les droits d’accès de l’utilisateur.

3.6 Fraud viewer

Un Fraud viewer peut uniquement visualiser les pages de configuration du module de détection des fraudes.

Remarque : Pour que ce profil utilisateur fonctionne correctement, vous devez cocher Fraud detection dans les droits d’accès de l’utilisateur.

3.7 Helpdesk admin

Le Helpdesk admin n’accès qu’à la page “Gestion des utilisateurs” dans le compte.

Pour plus d'information, aller aux autorisations utilisateur pour les différents profils.

3.8 Super-encodeur

Un Super-encodeur peut non seulement soumettre de nouvelles transactions, mais également réaliser des opérations de maintenance sur des transactions existantes. Il peut également télécharger en amont des fichiers de paiement et télécharger en aval des rapports de transaction.

3.9 Super-encodeur sans remboursement

Le Super-encodeur sans remboursement dispose des mêmes droits d’accès que le Super-encodeur, à ceci près qu’il n’est pas en mesure de procéder à des remboursements ni d’annuler des autorisations. Ce profil vous permet d’octroyer une permission en vue de procéder à des captures de données, sans cependant procéder à des remboursements ni supprimer des paiements.

3.10 Consulteur

Le profil consulteur est le profil idéal pour un comptable. Un Consulteur peut afficher ou solliciter les statuts et les rapports de transaction, mais ne peut rien modifier ni soumettre. Il s’agit d’un profil d’accès en lecture seule.

4. Types d'utilisateur

Nous disposons de 2 types d’utilisateurs :

- l’utilisateur back-office (= l’utilisateur ADM)
- l’utilisateur applicatif (= l’utilisateur API)

4.1 L'utilisateur Back-office (utilisateur ADM)

Un utilisateur back-office (utilisateur ADM) est un utilisateur ayant accès au module de gestion des comptes (back-office) via le site Internet.

Un utilisateur de back-office doit modifier son mot de passe tous les 90 jours. Il peut le faire via le lien “Mot de passe” dans le menu du compte.

4.2 Utilisateur API

Un utilisateur API (Application Program Interface) est un utilisateur spécifiquement destiné à être utilisé par une application en vue de procéder à des demandes automatiques à la plate-forme de paiement (téléchargement automatique en amont /en aval de fichiers, demandes de paiement directes, ...).

Même si pour un utilisateur API des différents profils d'utilisateurs sont disponibles, nous vous recommandons fortement de configurer cet utilisateur avec le profil "Admin". Si vous souhaitez limiter les droits pour l'entretien des transactions (remboursements, annulations, etc), vous pouvez toujours modifier le profil de l'utilisateur à "Encodeur".

Si vous n'êtes pas sûr, nous vous recommandons de choisir le profil "Admin", sinon, passez au profil de l'utilisateur pour plus d'informations.

Le mot de passe d’un utilisateur API ne doit pas être régulièrement modifié. Cette fonctionnalité est plus commode lorsque le mot de passe doit être intégré dans votre application. Nous vous recommandons cependant de modifier périodiquement votre mot de passe.

Afin de modifier le mot de passe d’un utilisateur API:

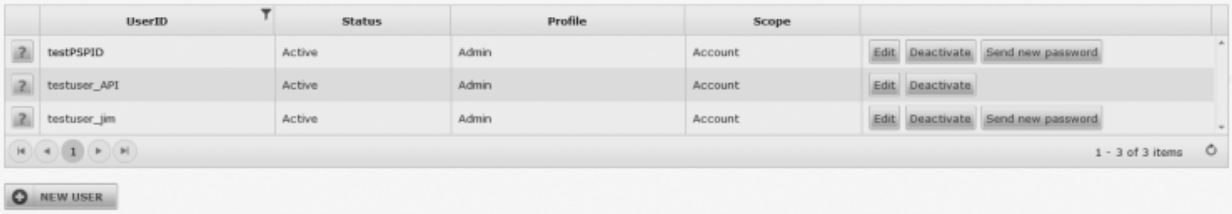
1. Choisissez le lien “Utilisateurs” dans le menu de votre compte
2. Cliquez sur le bouton “Changer le mot de passe” à côté du nom de l’utilisateur en question. Vous serez alors redirigé vers une page où le nouveau mot de passe de l’utilisateur peut être configuré. Lors de la création d’un utilisateur API, vous devrez également choisir le mot de passe sur cette page.

Pour des raisons de sécurité, les utilisateurs API n’ont pas accès au module de gestion du compte, c'est-à-dire qu’ils ne peuvent pas se connecter au back-office.

5. Gestion des Utilisateurs

Sur la page Gestion des utilisateurs, vous pouvez :

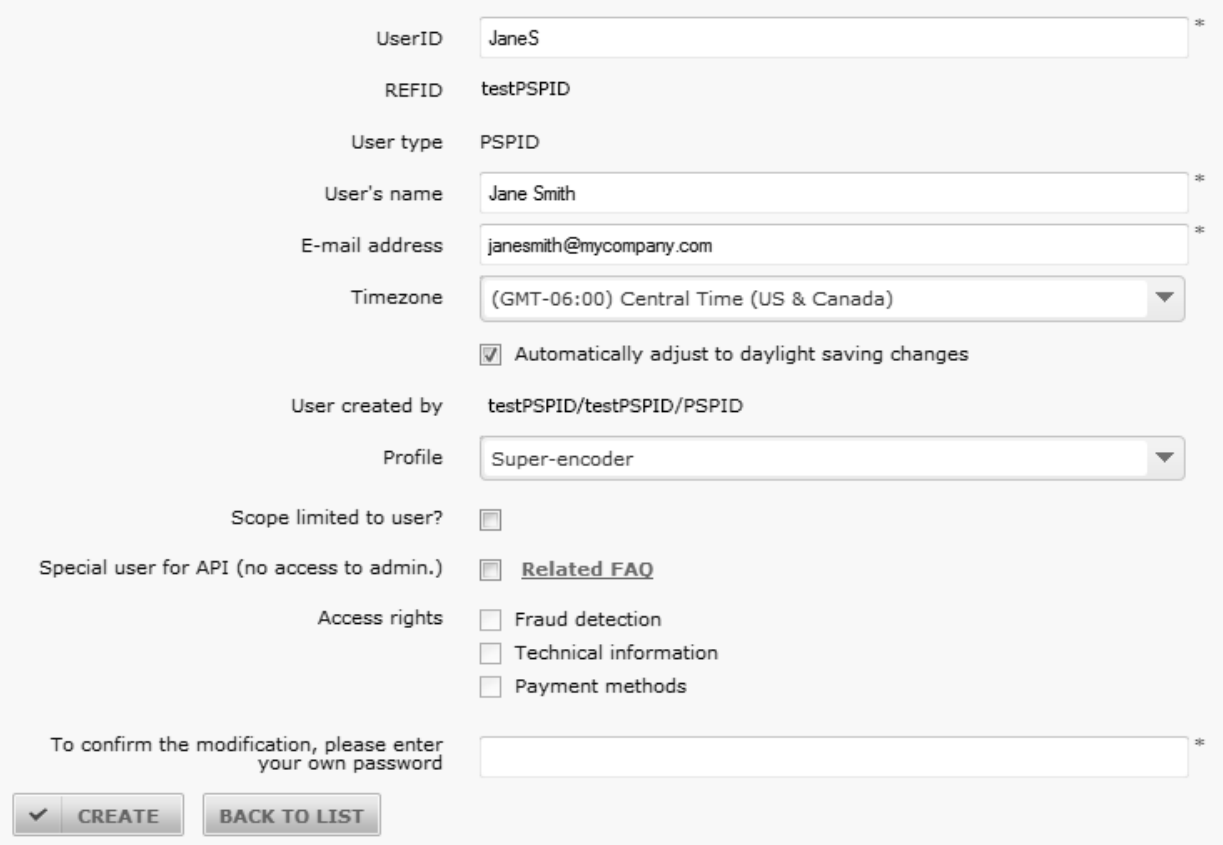
- créer de nouveaux utilisateurs
- gérer les mots de passe des utilisateurs
- désactiver des utilisateurs qui ne sont plus actifs au sein d'une société
- éditer des données à propos des utilisateurs



Le nombre d'utilisateurs autorisés est affiché dans la page de menu Utilisateurs. Dès que le nombre d'utilisateurs autorisés a été atteint, le bouton "Nouvel utilisateur" sera désactivé.

5.1 Créer un nouvel utilisateur

Vous pouvez créer un nouvel utilisateur en cliquant sur le bouton "Nouvel utilisateur" dans la page "Gestion des utilisateurs". Le système affiche un formulaire qui doit être complété en vue de soumettre un nouvel utilisateur.



5.1.1 Renseignements pre-initialisés

Le formulaire contient trois champs de données pré-initialisées :

- REFID : le nom de l'entité à laquelle le UserID est lié (par exemple pour un marchand : son PSPID).
- Type d'utilisateur : le type d'entité à laquelle le UserID est lié (par exemple pour un commerçant : "PSPID").
- Utilisateur créé par : le UserID de l'utilisateur créant ce nouvel utilisateur / son type d'utilisateur / son REFID.

5.1.2 Renseignements à propos de l'utilisateur

Les renseignements devant être complétés à propos de l'utilisateur sont les suivants :

- USERID : le UserID (nom d'utilisateur) du nouvel utilisateur (longueur minimale de 3 et maximale de 20 caractères, sans espace ni caractère spécial).
- Nom de l'utilisateur : le nom complet du nouvel utilisateur.
- Adresse E-mail : l'adresse électronique du nouvel utilisateur (si, par la suite, un nouveau mot de passe est généré pour cet utilisateur, il sera envoyé à cette adresse E-mail).

5.1.3 Fuseau horaire

Grâce à la création d'un utilisateur, automatiquement le fuseau horaire du PSPID est appliqué. Ensuite, l'utilisateur peut configurer le fuseau horaire de son choix.

Le fuseau horaire que l'utilisateur choisit est applicable pour toutes les pages de back-office où le temps est pertinente. De cette façon, l'utilisateur peut également afficher et télécharger des fichiers / rapports dans son fuseau horaire préféré.

En outre, le temps peut être automatiquement ajusté à des modifications de l'heure d'été, en sélectionnant cette option.

5.1.4 Profil

See User profiles.

5.1.5 Portée limitée à l'utilisateur

Cette option ne peut être configurée que pour les profils suivants :

- Encodeur
- Super-encodeur
- Super-encodeur sans remboursement

Si la case est cochée, les Encodeurs ne seront en mesure que de voir les transactions qu'ils ont saisies / initiées eux-mêmes et y accéder. Ils ne pourront pas voir les transactions saisies par d'autres utilisateurs ni y avoir accès.

Si la case est cochée, les Super-encodeurs et les Super-encodeurs sans remboursement pourront uniquement consulter les opérations de maintenance sur les transactions qu'ils ont saisies / initiées eux-mêmes et y accéder (à l'exception donc des activités de maintenance qui sont soumises par le biais du téléchargement de fichiers en amont). Ils ne pourront pas consulter les opérations de maintenance ni les transactions saisies par d'autres utilisateurs, ni y avoir accès ni les réaliser.

5.1.6 Case : Utilisateur API

Vous devrez cocher cette case si vous souhaitez créer un utilisateur applicatif (utilisateur API). L'utilisateur que vous créez ne sera utilisé qu'à des fins d'accès applicatif et non pour l'accès au back-office via le site Internet.

5.1.7 Cases : Accès spécifiques

Les modules d'accès "détection de fraude", "méthodes de paiement" et "informations technique" peut être activé si vous cochez les cases respectives.

Ces options ne peuvent être configurées que pour les profils suivants :

- Consulteur

- Admin
- Admin sans user management

Vous pouvez soumettre les paramètres d'utilisateur que vous avez saisis en cliquant sur le bouton “Créer”. Si l'une quelconque de ces informations a été erronément complétée, le système affichera un message d'erreur. Au lieu d'envoyer, à l'utilisateur récemment créé, son premier mot de passe par E-mail, le système affichera un écran précisant le mot de passe créé pour lui ; ce mot de passe pourra ensuite être communiqué au nouvel utilisateur.

5.2 Gestion des mots de passe

Vous pouvez envoyer un nouveau mot de passe à un utilisateur spécifique en cliquant sur le bouton “Nouveau mot de passe”. Ce nouveau mot de passe sera envoyé à l'adresse E-mail configurée dans les données de l'utilisateur.

Vous ne pouvez pas assigner un nouveau mot de passe à l'utilisateur avec lequel vous avez ouvert votre session, ni à l'utilisateur par défaut du compte.

Si l'utilisateur par défaut du compte a perdu son mot de passe, il ne pourra en demander un nouveau que via le lien “Mot de passe introuvable?” sur la page de login. A la page suivante, il devra compléter la PSPID et cliquer sur le bouton “Envoyer”. Un courrier électronique contenant un nouveau mot de passe sera envoyé à l'adresse E-mail administrative du compte.

Pour les utilisateurs API il n'y a pas de bouton “Nouveau mot de passé”. Pour changer le mot de passé d'un tel utilisateur, vous devez utiliser le bouton “Changer le mot de passe”, qui vous redirige vers une page où un nouveau mot de passe peut être configuré.

Pour plus de sécurité, vous pouvez également activer ou désactiver l'authentification à deux facteurs (2FA). Cliquez ici pour plus d'informations.

5.3 Désactiver des utilisateurs

Vous pouvez désactiver un utilisateur en cliquant sur le bouton “Désactiver” situé à côté de l'utilisateur. S'il a ce statut, il ne sera plus autorisé à se connecter à son compte et ne sera plus pris en considération pour le nombre d'utilisateurs autorisés.

Pour afficher une liste complète de tous les utilisateurs (tant actifs qu'inactifs), vous pouvez cliquer sur le bouton “Montrer les utilisateurs inactifs”.

Afin d'être conforme PCI et pour des raisons de sécurité, vous n'êtes /nous ne sommes pas habilités à supprimer des utilisateurs.

5.4 Editer les coordonnées de l'utilisateur

Pour modifier les coordonnées d'un utilisateur donné, vous pouvez cliquer sur le bouton “Editer” situé à côté de cet utilisateur. S'il s'agit de l'utilisateur du compte par défaut, seuls le nom et l'adresse E-mail pourront être modifiés.

5.5 Adresse IP

Afin de protéger de toute intrusion l'accès aux comptes Back Office des commerçants, les utilisateurs peuvent donner accès à une adresse IP spécifique (ou à une liste d'adresses IP) en enregistrant ces adresses dans le champ « IP Address » (Adresse IP).

Les utilisateurs doivent se connecter à l'aide de leur compte pour pouvoir configurer ce champ. Le champ « IP Address » (Adresse IP) se trouve dans « Login Access » (Accès à la connexion), sous l'onglet *Configuration > Users* (Configuration > Utilisateurs).

5.5.1 Restrictions en matière d'adresses IP pour les utilisateurs

Si leur adresse IP ne figure pas dans la plage définie, les utilisateurs ne pourront pas se connecter au Back Office.
Cependant, si le champ « IP Address » (Adresse IP) est vide, aucune restriction d'adresse IP ne s'appliquera pour la connexion au Back Office.
L'adresse IP de l'administrateur qui configure la plage IP doit aussi être incluse dans la plage définie. Sinon, l'administrateur recevra un

message d'erreur et l'adresse IP ne sera pas enregistrée.

5.5.2 Format et valeur de l'adresse IP

L'adresse IP doit aussi respecter un format strict :

- Elle doit être au format CIDR (par exemple: 212.166.204.28/32) ;
- Elle ne peut comporter plus de 512 caractères.
- Si vous souhaitez enregistrer plusieurs adresses IP, elles doivent être séparées par des points-virgules.

6. Login de l'Utilisateur

Pour vous connecter en tant qu'utilisateur, vous devez vous servir du formulaire de login (ouverture de session) avec les trois champs suivants : "UserID", "PSPID" et "Mot de passe".

Si le système affiche le formulaire d'ouverture de session contenant les deux champs PSPID et Mot de passe, vous pouvez passer au formulaire de login à trois champs en cliquant sur le bouton "User login" à côté du formulaire de login.

7. Suivi des Transactions de l'Utilisateur

Les données en matière de paiement d’une transaction comprennent un champ “encodé par”. Ce champ se compose de l’UserID/PSPID/type de l’utilisateur ayant encodé la transaction. Ce champ ne s’affiche pas pour les utilisateurs ayant été configurés avec une portée limitée à l’utilisateur dans les informations utilisateur.

Pour afficher toutes les transactions encodées par un utilisateur spécifique, choisissez l’utilisateur dans une liste déroulante (appelée ‘encodé par’) dans les critères de sélection approfondis pour “Historique financier” et “Gestion Transactions”.

8. Aperçu des Droits des Utilisateurs

R = lecture (droits de visualisation), W = écrire (droits de modifier /soumettre), **gras** = doit être configuré dans les informations utilisateur.

	Consulteur	**Encodeur**	**Super-encodeur**	**Super-encodeur sans rembour-sement**	**Helpdesk Admin**	**Admin**	**Admin sans user manager**
Renseignements en matière de langues /URL/devises pour le Contact Compte	R	R	R	R		R W	R W
Souscription Compte /option						R W	R W
Renseignements Facturation Compte						R	R
Méthodes de paiement	**R**					**R W**	**R W**
Utilisateurs					R W	R W	
Assistance	R W	R W	R W	R W	R W	R W	R W
Informations techniques	**R**					**R W**	**R W**
Journaux d'erreur	R	R	R	R	R	R	R
Module de Détection de fraude	**R**					**R W**	**R W**
Historique financier	R	R	R W	R W		R W	R W
Nouvelle transaction		R W	R W	R W		R W	R W
Gestion transactions	R	R	R W	R W		R W	R W
Nouveau fichier			R W	R W		R W	R W
Visualiser les fichiers			R W	R W		R W	R W
Rapports électroniques	R W	R W	R W	R W	R W	R W	R W
Alias Manager	R	R	R	R		R W	R W

8.1 Profils de détection de la fraude

Remarque: Pour que ces profils utilisateurs fonctionnent correctement, vous devez cocher "Fraud detection" dans les droits d'accès de l'utilisateur.

R = lire (droit de visualisation) W = écrire (droits de modifier/soumettre)			
	Fraud analyst	**Fraud manager**	**Fraud viewer**
Page de Détection de fraude	R	R W	R
Page de Détection de fraude : FDMA configuration & listes des risques	R	R W	R
Page de Détection de fraude : 3-D Secure configuration	R	R W	R
Page de Détection de fraude: Blacklists/Whitelists	R W	R W	R
Scoring details page	R	R	R
Scoring details page: fill dispute + Blacklists/Whitelists	R W	R W	-
Score details page: réviser transactions	R W	R W	-